Llaneros Solitarios; Hackers, la Guerrilla Informática

Autores: Fernando Bonsembiante / Raquel Roberti

Coleccion: Fin de Siglo

Director: Jorge Lanata

Editado el 4/94

Pirateado el 05/95

Gentileza de: Don Juan Caballero / Miriam Sf.

Corregido por sus autores el 30-11-96

I. ¿Qué es un hacker?

Unruly boys who will not grow up must be taken in band.	A los chicos rebeldes que no van a crecer Hay que ponerlos en una banda.
Unruly girls who will not settle down they must be taken in a band.	A las chicas rebeldes que no van a sentar cabeza Hay que ponerlas en una banda.
A crack on the head is what you get for not asking.	Un mamporro en la cabeza es lo que conseguís si no preguntás.
and a crack on the head is what you get for asking Barbarism begins at home	Y un mamporro en la cabeza es lo que conseguís si preguntás. El barbarismo empieza por casa.

MORRISEY, THE SMITHS

Las dos de la madrugada, Hannover, ciudad Alemana, estaba en silencio. La primavera llegaba a su fin, y dentro del cuarto cerrado el calor ahogaba. Hacia rato que Wau Holland y Steffen Wernery permanecían sentados frente a la pantalla de una computadora, casi inmóviles, inmersos en una nube de humo cambiando ideas en susurros.

- Desde acá tenemos que poder llegar. -murmuro Wau.

- Msé. Hay que averiguar cómo - Le contestó Steffen.

- El primer paso es averiguar el nombre de la máquina central.

- Probemos algunos. Siempre elijen nombres relacionados con la astronomía, ¿No?

- Tengo un mapa estelar: usémoslo.

Con el libro sobre la mesa teclearon uno a uno y por orden los nombres las constelaciones.

- "Acceso Denegado" -leyó Wau-; puta madre, tampoco es este.

- Quizá nos esté faltando alguna indicación. Calma. Pensemos. "set" y "host" son imprescindibles...

- Obvio; además, es la fórmula. Probemos de nuevo ¿Cuál sigue?.

- Las constelaciones se terminaron. Podemos intentar con las estrellas. A ver...¿Castor, una de las dos mas brillantes de Géminis?

- Set Host Castor -deletreó Wau mientras tecleaba.

Cuando la computadora comenzó a ronronear, Wau Holland y Steffen Wernery supieron que habían logrado su objetivo. Segundos mas tarde la pantalla mostraba un mensaje; "Bienvenidos a las instalaciones VAX del cuartel general de la NASA".

Wau sintió un sacudón y atinó a escribir en su cuaderno: "Lo logramos, por fin... Sólo hay algo seguro: la infinita inseguridad de la seguridad".

El 2 de mayo de 1987, los dos hackers Alemanes, de 23 y 20 años respectivamente, ingresaron sin autorización al sistema de la central de investigaciones aeroespaciales más grande del mundo.

- ¿Porque lo hicieron? -Preguntó meses después un periodista norteamericano.

- Porque es fascinante. En este mundo se terminaron las aventuras; Ya nadie puede salir a cazar dinosaurios o a buscar oro. La única aventura posible -respondió Steffen- está en la pantalla de un ordenador. Cuando advertimos que los técnicos nos habían detectado, les enviamos un télex: "Tememos haber entrado en el peligroso campo del espionaje industrial, el crimen económico, el conflicto este-oeste, y la seguridad de los organismos de alta tecnología. Por eso avisamos, y paramos el juego".

- El juego puede costar muchas vidas...

- ¡Ni media vida! La red en que entramos no guarda información ultrasecreta; en este momento tiene 1600 suscriptores y 4000 clientes flotantes.

Con esos datos, Steffen anulaba la intención de presentarlos como sujetos peligrosos para el resto de la humanidad. El hacking es una actividad no muy popular en Argentina, pero ya tradicional y muy convocante en el mundo. La palabra deriva de hack, hachar en ingles, y es el término que se usaba para describir la familiar forma en que los técnicos telefónicos arreglaban cajas defectuosas; el bueno y viejo golpe seco. La persona que realizaba esa operación era, naturalmente, un hacker.

En 1959 la denominación alcanzó a los estudiantes del Masachusetts Institute of Technology -el famoso MIT de los Estados Unidos-, que se reunían alrededor de la computadora IBM 407, una máquina a la que conocían mejor que a sus madres. En aquel tiempo, era común que ese aparato fallase por razones extrañas y las reparaciones, que solían ser esotéricas, incluían el casero método del impacto de costado, tan útil para tecnología valvular: el que nunca le pegó a uno de esos viejos televisores que tire la primera piedra. O demuestre su extrema juventud.

A poco de andar, los pioneros elaboraron sus propias reglas, que aún hoy se consideran básicas aunque no haya Colegio de Hackers ni Consejo Profesional. Las mas conocidas son las que Steven Levy dicta en su libro *Hackers, Heroes of the Computer Revolution* (Hackers, Heroes de la Revolución Informática), un clásico en la definición del hacking:

- El acceso a las computadoras -y a cualquier cosa que pueda enseñarte algo acerca de la forma en que funciona el mundo- debe ser total e ilimitado.
- Apelar siempre a la imperativa: ¡Manos a la obra!
- Toda información debe ser libre y/o gratuita.
- Hay que desconfiar de la autoridad. Hay que promover la descentralizacion.
- Los hackers deberán ser juzgados por sus hackeos, no por falsos criterios como titulos, edad, raza, o posición.

- En una computadora se puede crear arte y belleza.
- Las computadoras pueden cambiar la vida para mejor.

Las Primeras Truchadas

En 1876 Alexander Graham Bell creó el teléfono y el mundo cambió. Claro que no de un día para el otro. En los primeros tiempos, los norteamericanos vieron en ese aparato hoy imprescindible un juguete estrafalario para escuchar música, porque cuando Bell hizo la demostración pública de su invento transmitió por las lineas unos acordes que su ayudante, instalado exprofeso a cientos de kilómetros de distancia, tocó en un piano. Las personas no concebían entonces, que se le pudiera hablar a un aparato y les costó comprender que se trataba de hablar con otro por teléfono.

El inventor fundó la compañía Bell Telephone y se dedicó a producir y vender sus aparatos a pesar de la Western Union, empresa de telégrafos -esa que aparece en las películas de cowboys- que se esforzó por desmerecer a su nuevo competidor, el teléfono, y difundir las supuestas bondades de la telegrafía.

En enero de 1878 un terrible accidente ocurrió en Tarriffvile, Connecticut: un tren descarriló y causó cientos de heridos.

En medio de la confusión y los insuficientes auxilios, alguien llamó por teléfono a los médicos de la cercana Hartford, quienes acudieron de inmediato para atender las victimas. El extraño aparatejo obtuvo fama súbita y absoluta; la Bell no podía casi cumplir con las toneladas de pedidos que recibía. En el término de doce años pasó de Boston a Nueva Inglaterra; en 1893 estaba en Chicago y en 1897 en Minnesota, Nebraska y Texas. En 1904 ya se había desparramado por todo el continente.

A principio de los 60 casi todas las grandes empresas instalaban costosas computadoras que ocupaban habitaciones y hasta edificios enteros (mainframes); en las universidades se enseñaba el ABC informático. La Bell Telephone no fue ajena a esa renovación y los sistemas mecánicos y electro-mecánicos que habían reemplazados a las operadoras fueron desplazados por mainframes que controlaron de allí en adelante el flujo de las comunicaciones. Hasta que un día un técnico de la empresa le contó a un amigo cómo funcionaban los números de prueba que se utilizaban para chequear las lineas; eran *loops* (bucles de lineas entrelazadas), pares de números telefónicos.

- Si alguien llama al primer número de esos pares y otra persona se comunica con el segundo, terminan hablando entre sí -explicó el técnico-. Semanas mas tarde, Mark Bernay (el alias del amigo en cuestión) divulgó el secreto que, desde entonces, permitió realizar llamados de larga distancia gratis o pagando una comunicación local. En poco tiempo las líneas de Estados Unidos, se vieron pobladas de *phreakers*, tal como se llamaban a sí mismos los seguidores de Bernay. La palabra deriva de phreak, una extraña mixtura de *freak* (enfermo, o con cariño, bicho raro), phone (teléfono), y free (gratis). El grupo sostenía que la tecnología de las comunicaciones debía estar al alcance de todo el mundo y la única forma de lograrlo era que fuera gratuita.

Cuando los phreakers descubrieron que la tecnología de MaBell (como llamaban a la Bell Telephone) podía brindarles algo mas que el entretenimiento de llamar a sus amigos en Burkina Faso, decidieron controlar la red telefónica, desafío que requirió nuevos métodos. Si el hombre perdió el paraíso por la fruta prohibida del conocimiento, aquellos phreakers y estudiantes de ingeniería electrónica perdieron

la compostura ante los grandes ordenadores de MaBell: ni siquiera intentaron resistir la tentación, sólo sucumbieron de lleno a sus circuitos.

Así fue como todo comenzó

En 1961 la Bell Telephone denunció el primer robo de servicio telefónico: había detectado largas llamadas a un número de información de una zona aledaña. La investigación llevó a los inspectores hacia el State College de Washington, donde encontraron una caja extraña que denominaron *Blue Box* (caja azul) y que reproducía los tonos multifrecuencias de la compañía. Eran doce combinaciones de seis tonos maestros y -se suponía- secretos. Pero en 1954, la telefónica había publicado las frecuencias tonales en un jornal técnico que se distribuía entre su personal: Tarde cayeron en cuenta de que la leían todos los estudiantes y egresados de ingeniería electrónica. Los alumnos llamaban al número de información, y una vez comunicados entraba en acción la Blue Box, que emitía una señal para indicar a la central telefónica que ambos aparatos estaban en linea mientras los muchachos derivaban la llamada a un numero de larga distancia.

Diez años después, un articulo de Ron Rosembaum en la revista Esquire explicaba el funcionamiento de las cajas azules y quienes las usaban desde el inicio, entre ellos un enorme grupo de chicos ciegos que se comunicaban de costa a costa sin pagar un centavo.

De trampear a MaBell con llamadas de larga distancia para hablar con un amigo y hacer lo mismo para hablar con una computadora había un solo paso, y los pioneros del hacking lo dieron sin hesitar. Hasta ese momento la penetración en las computadoras ajenas por intermedio del teléfono era muy nueva y aun no tenía nombre, de modo que Rosembaum la llamó *computer freaking* para distinguirla del *phreaking telefónico*.

Hecho en Casa

Cuando Oak Toebark leyó el articulo de Rosembaum decidió fabricar sus propias cajas azules, venderlas en sociedad con su amigo Berkeley Blue y, con el dinero que ganaran, comprar una computadora igual a la que operaba en las oficinas de Hewlett Packard. Si bien tuvieron un relativo éxito, las ganancias no alcanzaron.

- Voy a construir una -aseguro Oak ante la perplejidad de Berkeley- .

Ocupó casi un año de su vida en lograr su ordenador personal (nunca tan bien aplicada la definición) y cuando consideró que estaba listo, en 1976, lo presentó al *Homebrew Computer Club* (Club de Computadoras Caseras), del que era miembro.

- La tienda nos hizo un pedido de cincuenta mil dólares- Anunció a los pocos dias Berkeley, encargado de las ventas.

Steve Wozniak (Oak) y Steve Jobs (Berkeley) fundaron la Apple Computers y en 1977 presentaron en la Feria Informática de la Costa Oeste, en los Estados Unidos, la Apple II, que superaba a la anterior por la posibilidad de usar disco flexible. Wozniak y Jobs iniciaron así una verdadera revolución social, ya que sus máquinas permitieron el acceso popular a datos y programas. Uno de los primeros videos promocionales de Apple mostraba un empleado de la empresa que decía frente a cámara: "Fabricamos

un aparato que da a la gente el mismo poder sobre la información que las grandes corporaciones y el gobierno poseen sobre la gente". Ese fue el nacimiento de Apple, una de las dos empresas que hoy disputan el mercado de la computación personal. La otra, IBM (International Business Machines), lanzó su primer *Personal Computer* (PC) en 1981, 6 años mas tarde. El segundo modelo de Apple fue la primera computadora personal tal como se las conoce ahora. La fabricación en serie permitió que miles de personas se introdujeran en la computación, ya que el costo no era demasiado alto.

Hasta ese momento el movimiento hacker estaba constituido por unos pocos que podían trabajar en una gran empresa o estudiar en una universidad. A partir de allí lo que era el patrimonio de una élite se amplió a un mundo de chicos y chicas curiosos, marcando el inicio del hacking casero de hoy en día: Aquellos que dedicaban algunos ratos a jugar invirtieron horas de sus vidas a intentar diferentes cosas aplicando los conocimientos adquiridos mediante el phreacking.

Juegos de Guerra

Durante 1983 se vivieron horas de extrema tensión en la central de la NORAD en la montaña Cheyene, Colorado, Estados Unidos. Los altos mandos militares observaban con atención las pantallas gigantes que dibujaban el recorrido de 2400 cohetes atómicos enviados por los rusos contra el territorio norteamericano. La información provenía de una inmensa computadora, la WOPR (War Operation Plan Response, Responsable del plan de Operaciones de Guerra).

- Tiempo estimado de impacto, 20 segundos -anunciaba una voz femenina.

Parecía que finalmente el mundo se había sumergido en la guerra termonuclear global. La decisión de contraatacar dependía del presidente de los Estados Unidos, quien decidió esperar. El tiempo se estiró como un chicle. En el segundo veintidós, todos supieron que habían vivido una fantasía.

David Lightman, estudiante secundario, había ingresado casi por casualidad con su computadora hogareña IMSAI, y a través de una conexión telefónica, al sistema de la NORAD apelando al listado de juegos disponibles. Una vez habilitado, comenzó el diseño táctico de la guerra, que la computadora siguió desarrollando aun después de que David cortara la comunicación.

La historia no es mas que el argumento de Juegos de Guerra, película de John Badham que popularizó el hobby del hacking y provocó una verdadera invasión de curiosos en los sistemas informáticos.

El filme no sólo fue un absoluto éxito taquillero, si no que también abrió los ojos y la cabeza de miles de jóvenes apasionados por la computación. A partir de entonces, las mainframes de las grandes empresas, militares o del gobierno, así como las redes informáticas, fueron el blanco predilecto de los hackers, ansiosos por descubrir nuevas fronteras y develar todos los secretos guardados celosamente por esas máquinas. En poco tiempo accedieron a conglomerados de computadoras y redes del mundo y comenzaron a viajar por ese espacio electrónico.

La película estaba muy bien documentada y presentaba técnicas reales, como el uso de un programa que buscaba en forma automática números telefónicos donde atendiera un módem. Hoy en el mundo hacker a un programa similar se lo llama *Wardialer* o "Discador tipo Juegos de Guerra".

¿Quién es ese hacker?

- No sé leer ni escribir y me alegro de ello.

- Jamás leí a Freud, no sé quién es Nietzsche, no me interesa Borges.

- No sé nada de computación ni me interesa.

Nadie en su sano juicio pronunciaría ninguna de las primeras frases en público. La tercera, aunque igual de temerariamente necia, se escucha a menudo. Los impuestos son controlados por computadoras, las tarjetas de crédito dejan el rastro de su titular en un ordenador remoto, las llamadas telefónicas son almacenadas en una mainframe. Cualquier vendedor puede seguir las pistas que cientos de ciudadanos dejan a diario en decenas de computadoras para averiguar qué tipo de cosas puede ofrecer a cada quien, e incluso se puede perder la oportunidad de sacar un crédito porque hace diez años se dejó impaga una multa de tránsito en alguna parte. Parece que las computadoras rigen las vidas humanas; Por lo tanto, es sencillo deducir que quien maneje esas máquinas podrá tal vez dominar al hombre. Un organismo oficial armado de un potente ordenador que siga los movimientos de una persona puede convertirse en pesadilla, al estilo de 1984, de George Orwell. Si el hombre no sabe cómo funciona ese control nada podrá hacer para evitarlo. No es de extrañar entonces que a las grandes corporaciones y a los gobiernos les interese que la ciudadanía sepa lo menos posible del tema.

El *Chaos Computer Club*, que agrupa hackers alemanes, divulgó las cifras de contaminación nuclear posteriores al accidente de Chernobyl, que el gobierno ruso guardaba bajo siete llaves. La difusión de secretos de ese tipo convierte al hacking en peligroso ante los ojos del establishment que -ni lerdo ni perezoso cuando de cubrir sus espaldas se trata- comenzó a dictar leyes represivas en los Estados Unidos, Holanda, Inglaterra, y Chile, para lo que se conoce como "Delitos informáticos", castigados con fuertes multas y años de prisión.

Pillos, audaces, marginales, delincuentes, bohemios, artistas, drogadictos, románticos, espiás y también genios son algunos de los tantos adjetivos que se han usado -y se usan- en el mundo para definir a los hackers. Un buen cóctel de todos ellos daría una mezcla explosiva y, quizá, una idea global del hacker típico.

Desde sus inicios hasta el presente, los hackers no solo son lo que son: También generaron imágenes en los ajenos a ese mundo tecnológico que corre paralelo al de la rutina cotidiana.

Garteh Branwyn sostiene, en su introducción a *Secrets of a Super Hacker* (Secretos de un Super Hacker, escrito por The Knightmare), que el pueblo norteamericano mezcla realidad y fantasía para configurar distintos modelos de hackers de acuerdo a sus propios deseos. Son "científicos independientes" cuando se asocian a los estudiantes del MIT que alcanzaban a ver la promesa de una vida distinta del otro lado de la pantalla y que peleaban en el límite de la tecnología y sus propios cerebros. Pueden convertirse en "cowboys" si se quiere reactualizar el mito americano de individualidad y supervivencia en una frontera violenta y sin ley. Pero cuando la red Internet quedó paralizada temporalmente por un programa que introdujo un hacker, se convirtieron en "tecnoterroristas", una visión acentuada por los medios de prensa que presentaron el caso como una catástrofe. Y si entra en juego el "vasto océano de internet" también dan el perfil de "piratas" relacionados con el comercio de información. Hackin Bey, teórico anarquista, destacó la posible

similitud entre una nueva cultura nómada y anarquista -producto de la rapidez en los cambios del mundo tecno- con la existente en el 1700, época de verdaderos piratas.

Bruce Sterling, escritor Ciberpunk desarrolló la idea mejor que nadie en su novela Islas En la Red: Los hackers forman una comunidad de una isla para escapar de las leyes que restringen su actividad y se dedican a la compra-venta de información. Son piratas en el mas puro sentido del término y el título de la versión en Portugués -piratas de datos seria su traducción- da la real dimensión del argumento.

Los Tiger Team (Equipo de tigres) alquilan su conocimiento para chequear las fallas de seguridad de diversos sistemas, por lo que son vistos como "informantes de seguridad". Y por último pero no menos importante, está la idea de que son "cyborgs", mezcla de robot y humano, los primeros en comprender que la especie esta cerca de desaparecer en el cyberespacio, donde se borraran los límites entre la máquina y el hombre. Es una figura más política que pelea el poder con el gobierno para que no domine ese nuevo mundo.

La comunidad hacker tiene otra visión de sí misma y comparte muy pocos elementos de estas fantasías populares. El *New Hacker's Dictionary* (Nuevo diccionario del hacker, una compilación de las palabras usadas por ellos, a cargo de Eric Raymond) los describe como inteligentes, intensos, abstraídos e intelectualmente abiertos. Se interesan en cualquier sujeto que les pueda proveer estimulación mental y es común que tengan una afición externa al hacking, en la que se desenvuelven mas que competentemente.

Les encanta el control pero no en forma autoritaria sino sobre cosas complicadas, como las computadoras. Se apasionan por lograr que esas máquinas sean instrumentos de lo interesante, siempre y cuando se trate de sus propias ideas y no de una orden de alguien. No les gustan las pequeñas tareas diarias que llevan a mantener una existencia normal; por ello, si bien son ordenados en sus vidas intelectuales, son caóticos en el resto. Prefieren el desafío del conocimiento a una recompensa monetaria por un trabajo.

Curiosos Profesionales

La casa es una vieja construcción en el centro de Buenos Aires. El Chacal baja del ascensor andando sobre patines, abre la puerta y saluda. Tiene el pelo largo, viste ropa de estilo militar y cuelga sobre su espalda una mochila con luz intermitente "para que no me lleven por delante los idiotas de los autos", explica.

Es un pionero del hacking en el país.

- ¿Qué motiva a un hacker?

- Muchas cosas, pero sobre todo la curiosidad. Si en el mundo todas las personas fueran conformistas, no avanzarían. Si fueran todos curiosos o aventureros, se extinguirían. El equilibrio esta en la existencia de un quince o veinte por ciento del segundo grupo.

- ¿Y para qué sirven?

- El curioso cumple un rol de vanguardia: muere intentando descubrir algo o permite el acceso del resto a una nueva situación. Cuando vé algo distinto, se pregunta qué habrá mas allá y no se detiene hasta averiguarlo. Asume el riesgo solo, pero si le va bien se benefician los demás.

- ¿Cómo?

- Una vez que tiene la respuesta vuelve al grupo con la novedad, los hace partícipes de su descubrimiento y de los beneficios que ello acarrea. Siempre habrá algo que lo haga regresar a la comunidad: un amigo, una novia, puede ser cualquier cosa. Este proceso es tan antiguo como la humanidad, sólo que ahora se usa una nueva herramienta, la computadora, en este caso para el cerebro.

- Descripto en esa forma, ¿No se constituye en uno de los últimos costados románticos de la década?

- Si, somos románticos. Recuerdo que nos gustaba decir que eramos "Los caballeros de las redes". Curiosidad y romanticismo son solo dos de las tantas características que distinguen a los hackers de los demás mortales. Por la profunda dedicación que brindan a su hobby, es fácil asociarlos y hasta confundirlos con aquellos "tragas" del secundario.

Guy L. Steele, en *The New Hacker's Dictionary* (Nuevo diccionario del hacker) observa: "Una de las razones de esta asociación es que un hacker realmente dedicado a su tarea no hace otra cosa mas que dormir, comer, y hackear. Algunos se levantan a la hora de cenar, y se acuestan después del desayuno. Contradiciendo la creencia popular de que son personas solitarias, los hackers tienen amigos. Amigos humanos. Por el tiempo que se comparte y por el trabajo en red, la computadora hace posible una nueva modalidad de comunicación, que resulta mejor que el teléfono y el correo juntos.

- Cuando me casé envié invitaciones a mis amigos hackers, pero como me conocían por mi login (Identificacion del usuario) y no por mi verdadero nombre las leyeron y se preguntaron "¿Y estos quiénes son?". Tengo otro amigo con el cual conversé durante años a través de una red y no supe que era sordo hasta que nos encontramos frente a frente. Esto demuestra que en el hacking no importa como sos o como te llamás, sólo interesa lo que pensás y decís". "La computadora unifica, socializa. Nadie se pregunta si sos negro, verde, o amarillo", escribió el norteamericano Emmanuel Goldstein hacker prócer y editor de la revista *2600, The Hackers Quarterly*.

Las circunstancias en que el hacking debe ser llevado adelante lo convierten en una actividad exigente. En general es un hobby nocturno que se realiza después de las obligaciones diarias -estudiar o trabajar-, porque para utilizar la computadora de otra persona o de una empresa, debe esperarse a que esté desocupada. En los horarios en los que el resto de la gente se encuentra para disfrutar del tiempo libre, ellos prefieren estar ante una PC intentando alguna conexión. Pocas veces se reúnen para sesionar en grupo: El manejo de un ordenador es individual y requiere de una gran concentración. Deben tener profundos conocimientos técnicos, lo cual no es sinónimo de haber estudiado una carrera relacionada con la computación ni haber asistido a cursos especializados; Lo que saben es producto de una experimentación permanente ante una pantalla, de la lectura de cuanto manual cae sobre sus escritorios y del ingenio, la picardía y la lógica para saltar las barreras de seguridad que presentan los sistemas. A veces pecan de soberbios.

- Si tenés cincuenta mil dólares no los llevás en el bolsillo ni andás por la calle con ellos, ¿no?, porque no querés que te roben. Bueno, esto igual: Si no querés que te usen la computadora protegéla - dice Opii, otro hacker nacional.

- Alguien que usa la computadora para su trabajo no tiene porqué saber tanto de computación como los hackers. ¿Debe correr el riesgo permanente de que algún día le desaparezcan o se estropeen sus archivos?

- ¿Vos nunca hacés copia de seguridad?

No perdonan la ignorancia de un oficinista ni la ingenuidad de una secretaria. La naturaleza de las excursiones que realizan los lleva a vivir en situación de riesgo cotidiano, ya que en cualquier momento pueden ser descubiertos (aunque no siempre identificados, ya que todos utilizan alias). La mayoría se inclina por la música heavy metal y las emociones fuertes, como el aladeltismo o el salto en paracaídas. Constituyen un grupo quizá marginal y que en sus orígenes demostró su desprecio por los códigos sociales usando pelo largo, vaqueros y sandalias en cualquier circunstancia. Hoy las reglas del aspecto no son tan estrictas y se permite cualquier vestimenta, siempre y cuando haya un toque estrafalario.

Opii parece un muchacho común: tiene el cabello corto, y llega a las citas con vaqueros, zapatillas y una remera. Pero elabora una pose llamativa: Habla poco y en forma pausada, sonríe menos, contesta ambigüedades, y deja la sensación permanente de que oculta algo esencial. Uno de sus amigos, Janx Spirit calza botas, usa campera negra de cuero, lleva el pelo largo pero con las sienes rapadas y se deja crecer la uña del pulgar izquierdo.

Cuando se juntan mas de tres se los puede confundir con una banda de rock; algunos de ellos en verdad tocan instrumentos musicales.

Son pocos los que pasan los 25 años: la franja mas amplia va de los 17 a los 23 y por lo general estudian carreras relacionadas con computación, matemáticas, ingeniería o electrónica. Los que llegan a los treinta sin abandonar la actividad mantienen una actitud adolescente y alternan entre las responsabilidades del mundo adulto y los juegos de la infancia. Emmanuel Goldstein comenzó a hackear cuando tenia diecisiete años; hoy anda por los treinta y es uno de los referentes mas visibles del hacking norteamericano.

- ¿Trece años no es mucho tiempo para hacer siempre lo mismo?

- La tecnología cambia permanentemente: no hay manera de aburrirse, siempre encontramos un nuevo juego. Ser hacker es tomarse todo el tiempo del mundo para jugar e inventar. En general, entre los veinte y treinta años la mayoría deja de ser hacker porque piensa en sentar cabeza y decide que no tiene tiempo para jugar. Es una pena.

De Hippies a Empresarios

El hacking nació como un movimiento tecnológico antisistema, con raíces en los que revolucionaron la década del 60: la anarquía (la YIPL, una linea del radicalizado Partido Internacional de la Juventud, publicó la primera hoja secreta de divulgación del *phreaking*); el hippismo, de donde toma el uso frecuente de drogas; la contracultura, que le marcó el gusto por la música heavy metal. Con estos datos

no es difícil concluir que la mayoría de los lideres iniciales del hacking tienen hoy edad y onda de ex hippies y que, como dice Goldstein, ya sentaron cabeza.

Claro que no todos lo hicieron de la misma manera. Bill Gates y Paul Allen integraban la *People Computer Company* (PCC), cuyo objetivo era difundir conocimientos sobre las mainframes y desmitificarlas. En los finales de los 70 estaban sentados delante de una PC Altair 8800, la primera computadora personal exitosa. Habían gastado 395 dólares en ella pero no podían utilizarla porque carecía de software.

- ¿Porqué no probamos con el BASIC? - preguntó Allen

Puestos a pensar, adaptaron el *Beginners All-Purpose Simbolic Instruction Code* (BASIC), lenguaje de programación, para la Altair. Esta fue la semilla de la poderosa Microsoft: pocos años después Gates y Allen eran multimillonarios gracias a un contrato con IBM para desarrollar el DOS, sistema operativo que se vendió con la IBM PC original y resultó un éxito comercial fuera de toda previsión. Algunos, sin tantas aptitudes para los negocios duros, optaron por ganarse el pan con el sudor de su mente. Knightmare, alias del autor de *Secretos de un Super Hacker*, divulgó en su libro los conocimientos necesarios para convertirse en un hacker de ley. "El hacking es el séptimo crimen computacional (los 6 anteriores son robo de dinero, sabotaje, robo de hardware, de software, de información y espionaje industrial). Quien elije el hacking prefiere no cometer los otros; sus motivaciones son el ansia de saber, adquirir conocimientos, y divulgar la información obtenida", predica, aunque reconoce que las situaciones no siempre son tan puras. "Muchos hackers usan su talento para hacer negocios: Robar, defraudar mediante tarjetas de créditos, o alquilar sus servicios, por ejemplo, a los investigadores privados para averiguar datos de y para sus clientes", afirma.

En esto se encuadra el espionaje, no solo industrial, si no también el de algunas áreas de gobierno. Knightmare sostiene que "constituyen un descrédito para la comunidad; los verdaderos y vocacionales desprecian esta línea de trabajo. Pueden perdonar y entender que se haga una vez, pero si la actitud es reiterada lo que se vende es la integridad".

Bill Landreth, autor de *Out of the Inner Circle* (fuera del círculo interior), se inclinó por escribir sobre un caso real, el suyo. Con el alias de Cracker creó -junto a Alpha Hacker, Mandrake, y otros- un grupo de elite, el Inner Circle (Circulo Interior), para intercambiar información utilizando como lugar de reunión la red Telemail de GTE. De su experiencia concluyó que existen cinco categorías de hackers:

- Los **novatos**, que ingresan en el mundo del hacking con posterioridad a Juegos de Guerra, se cansan pronto y abandonan;
- los **turistas**, que insisten en sus intentos hasta entrar en un sistema y luego lo abandonan para hacer lo mismo con otro;
- los **estudiantes**, solo interesados en conocer y aprender a manejar el sistema en el que ingresan;
- los **crashers**, que acceden a una maquina con la sola intención de producir daño;
- los **ladrones**, que buscan el beneficio económico y, generalmente, forman parte del personal de la empresa involucrada en el robo o estafa.

Hoy su libro se considera tanto manual del hacking como anti, ya que el autor no sólo describe métodos sino que también se muestra arrepentido y da soluciones para los administradores de sistemas.

Nombres Verdaderos y otros Peligros

Peter Gabriel definió que una máscara sirve para ocultar la cara pero es mas útil para mostrar lo que realmente hay en la persona que la usa. Al elegir su alias, nombre de guerra o handle, un hacker tal vez muestra parte de su verdadera y oculta personalidad.

Eric Corley leyó la distopia *1984*, de George Orwell, y decidió ser Emmanuel Goldstein, el "enemigo del pueblo", líder de un quizás imaginario movimiento de rebelión en contra del gobierno totalitario y opresor. Goldstein se ve a si mismo como ese personaje, alguien que a través de una revolución (pacifica en su caso) se opone al sistema y pretende liberar a la gente de la opresión de las multinacionales y grandes corporaciones.

1984 es una fuente inagotable de términos para el mundo hacker: Las grandes corporaciones -la policía es una personificación- son llamadas *Big Brother*, el Gran Hermano. Los hackers suelen citarlas con las frases "el gran hermano te está observando" o "policía del pensamiento, queda arrestado", tan repetidas en el texto de Orwell.

"*Galactic Hacker Party*" y "*Hacking at the end of the universe*" son los nombres de dos fiestas que se hicieron en Holanda. Ambas hacen referencia a la obra de Douglas Adams, autor de la trilogía (hasta ahora, trilogia de cinco libros), de la *Guia del Autoestopista Galáctica*, el segundo de cuyos libros se titula *El Restaurante del Fin del Mundo* (según las editoriales españolas, esas son las traducciones de Hitchicker's Guide to The Galaxy y The Restaurant At the End of The Universe). Un hacker local se llama Janx Spirit, al igual que la bebida mas poderosa del universo; según la susodicha Guia, con la Janx Spirit se prepara el *Pangalactic Gargle Blaster*, trago reventador de gargueros que según los holandeses, se iba a servir en la Galactic Hacker Party como parte del programa.

Count Zero, Wintermute y Case son alias copiados de la novela mas conocida de William Gibson, *Neuromante*, y sus secuelas. El autor presenta la palabra cyberespacio, con la que actualmente se denomina el conjunto de las redes, y relata la vida de un cowboy de consola (Case) en esa dimensión desconocida. Su trabajo es buscar información penetrando en los sistemas informáticos ajenos: es un hacker aunque la palabra jamás aparece en el libro. A pesar de que Gibson no tenia ni idea de computación, de alguna forma logró plasmar los arquetipos del movimiento hacker. El nombre mismo, Neuromante, es una mezcla de nigromante, mago, y neuro, relativo al sistema nervioso. El Neuromante es un mago que hace su magia mediante neuronas, su inteligencia; en vez de usar teclado y monitor interactúa con la máquina a través del cerebro conectado a la red, una sensación que a veces comparten algunos hackers que están casi físicamente conectados con la computadora.

Hagbard, el primer hacker reclutado por la KGB, para espiar los secretos de Occidente, tomó su seudónimo de la trilogía *Illuminatus!*, de Robert Shea y Robert Anton Wilson. Illuminati era el nombre de una secta secreta que no reparaba en asesinar para conseguir sus fines; el héroe que se le opuso era Hagbard Celine.

Pero a la hora de elegir una identificación, también valen los motivos mas diversos. El Chacal dice que su nombre se debe a que siempre se sintió un lobo solitario. Opii saco su handle de una remera que

diseñó un amigo suyo. Algunos se acercan a la caballería como Knight Lightning (El Caballero Relámpago) o The Knightmare (El caballero pesadilla). Fry Guy (el tipo frito), se inspiró en una propaganda de McDonald's. Otros prefirieron dar cierta idea de ilegalidad en su alias. Tales los casos de Truchex y Doctor Trucho. Este último marca una tendencia en el mundo hacker: ponerse títulos inventados para dar la idea de importancia. Tampoco podía faltar, claro, un ídolo de multitudes como el Capitán Piluso.

Una buena fuente de handles es la misma tecnología, pero siempre con un toque literario. En Buenos Aires, actúa Logical Backdoor: un *backdoor* es una puerta trasera para entrar en un sistema sin usar los procedimientos legales u oficiales, y en general la usa el programador para hacer algún tipo de mantenimiento. En los Estados Unidos, uno de los hackers mas famosos, compañero de Goldstein, es Phiber Optic (Fibra optica), el componente más moderno de las lineas digitales de telefonía. En la revista *2600* colabora Silent Switchman: Un *switchman* es el encargado de manejar los interruptores telefónicos, un técnico especializado.

Estos seudónimos a veces reemplazan al nombre original. Hasta sus amigos mas íntimos llaman Emmanuel a Eric Corley y nadie, salvo las autoridades de la cárcel y su madre, recuerda que Phiber Optic es Mark Abene.

Las organizaciones de hackers eligen sus nombres con criterios similares. La primera que se conoció en el país fue PUA, Piratas Unidos Argentinos, y en estos días funciona -aunque ellos prefieren considerarse "un grupo de amigos"- una segunda, HBO, un homenaje a las (malas) traducciones del canal de cable HBO Olé. Phrack inc., Anarchy inc., American Tone Travelers, Hackers of America y Phortune 500 son algunos de los grupos hackers de Estados Unidos que, aparentan ser grandes corporaciones. Otros simplemente prefieren mostrarse como malos, malísimos: League of Doom (los enemigos de superman según la historieta), Bad Ass Mother Fuckers (algo así como reverendos hijos de puta), Chaos Computer Club de Alemania (Club del Caos) o Masters of Deception (Maestros del Engaño).

Ética

- Sigo creyendo que la información y la tecnología deben ser libres, estar al alcance de cualquiera - opina El Chacal.

- El gobierno dice "confíe en nosotros" y nosotros decimos "de ninguna manera" - sostiene Goldstein.

- En los datos de un censo yo no voy a leer lo mismo que un político. Entonces ¿porqué esas cifras no están a mi alcance? - se pregunta Logical Backdoor.

Liberar la tecnología de los controles del estado y de la industria y ponerla al alcance de todos -algo que obviamente no sucede en este universo propietario y comercial- es el objetivo reconocido aún hoy por la mayoría de los hackers y la razón que esgrimen siempre que necesitan justificarse. Es simplemente el primer punto de aquellas reglas de Levy: "El acceso a ordenadores y cualquier cosa que pueda enseñar como funciona el mundo debería ser ilimitado y total (mira pero no toques)", que aún rige a los hackers auténticos y vocacionales, sobre todo el paréntesis. No tocar ni alterar los datos de los sistemas en que ingresan es una cuestión indiscutible y se juegan el honor y la maestría en ello. Forma

parte de un código ético que casi todos se afanan por respetar y que los diferencia de los que utilizan la computadora como herramienta para concretar un delito como estafa, robo o defraudación.

A pesar de los esfuerzos de estos llaneros solitarios, y en buena medida por responsabilidad de los medios de comunicación es común que se llame hackers a todos por igual, confundiendo actividades y objetivos. La mezcla no es en absoluto insensata, ya que unos como otros aprovechan las debilidades de los sistemas operativos, las fallas en la seguridad, la filtración de información o la ingenuidad de los operadores y clientes en el momento de elegir una contraseña (password), para ingresar subrepticiamente en esos sistemas.

Cuando se produjo el robo de una caja fuerte en la sede de la OTAN, los agentes federales descubrieron que el ladrón adivinó la combinación cuando vio una foto de Sofía Loren sobre la caja: las medidas de la actriz eran la clave. Michael Synergy (quien cambió su apellido legal por su alias) ingresó a mediados de los 80 -tal como era de costumbre en esos días- en la agencia de crédito nacional estadounidense TRW, que contiene información sobre unos ochenta millones de ciudadanos, con la idea de husmear en el fichero del entonces presidente Ronald Reagan. En su vagabundeo por los registros descubrió algo que le llamo la atención: cerca de setecientas personas con historiales de crédito extraños que parecían tener una tarjeta especifica. Synergy sospecho que se trataba del programa de protección de testigos del gobierno y notificó al FBI del agujero negro en la seguridad del sistema, ya que allí se encontraban los nombres y las direcciones de los protegidos. Lo hizo a riesgo de tener que afrontar las consecuencias de su ingreso ilegal en la TRW. La diferencia entre una actitud y otra es lo que delinea ese código ético de los verdaderos hackers.

En abril de 1990 los Estados Unidos organizaron un debate a través del WELL (*Whole Earth 'Lectronic Link*, una red con base en California) para responder a tres preguntas sobre el tema: ¿Es un delito ser hacker?, ¿Cuáles son los limites de libertad y la propiedad privada? y ¿existe una ética del hacker?

A lo largo de once días, se intercambiaron algunas de estas intervenciones:

Adelaide *(Seudónimo; hoy es programadora de una corporación estatal): "Las computadoras son poder, y el contacto directo con el poder puede sacar afuera lo mejor o lo peor de una persona. Es tentador pensar que cualquiera que tome contacto con la tecnología puede lograr una enorme inspiración, pero, ay, ay, eso no es así".*

> ***Lee*** *(Felsestein. Diseñó la computadora "portátil" Osborne 1 y cofundó el Homebrew Computer Club): "En algún lugar existe la Dínamo de la Noche, el ultramecanismo que espera ser soñado y que nunca podremos lograr realmente, pero que se hace realidad en algún lugar cerca de esos juegos mentales. Cuando vuelvo a emerger a la luz del otro día con el dibujo sobre el papel -y sabiendo que aunque vuelvan a aparecer las cosas nunca serán las mismas- yo sé que estuve en el lugar donde van los artistas. Para mí éso es ser hacker: trascender las custodias y engancharse en la creatividad para el propio beneficio, pero también crear efectos objetivos".*
>
> ***Emmanuel*** *(Goldstein): "¿Llamar a alguien por teléfono no equivale a golpear la puerta de esa persona?. Error. Cuando alguien contesta el teléfono, vos estás fuera de su casa; lo mismo con el contestador o una PC conectada a la línea. No es correcto violar la*

privacidad, y el escudriñamiento electrónico no es igual a violarla y entrar. La clave está en que mucha gente no sabe cuán sencillo es para los demás invadir su privacidad electrónica y espiar sus tarjetas de crédito, sus cuentas de teléfono, sus prontuarios, etcétera. Si tuviéramos un público educado, pensante, quizá nunca se hubiera permitido que llegaran a existir las bases de datos inmensas, tan comunes hoy en día. Los hackers podemos caer en una trampa: descubrimos los agujeros del sistema y luego nos culpan por esas fallas. La casa de un particular es mucho menos interesante que el Departamento de Defensa; son las instituciones las que tienen acumuladas montañas de datos sin nuestro consentimiento".

***Barlow** (John Perry. Ganadero retirado, ex presidente de la junta republicana de su condado y letrista de Grateful Dead): "En Wyoming las armas de fuego forman parte del mobiliario y es común ver una calcomanía de contenido politico: "Témele al gobierno que teme a tu pistola". Asumiendo el riesgo de que parezca exagerado, yo digo: "Témele al gobierno que teme tu computadora".*

***Dave** (militar de West Point retirado): "El público está en ascuas y lleno de temor frente a los misterios que manejan los nuevos sacerdotes de la nueva religión norteamericana: las computadoras. Reacciona del mismo modo como toda vez que el miedo lo lleva a enfrentarse con lo desconocido: Desea destruirlo, quemarlo en la hoguera. Los hackers son como los cristianos primitivos: Cuando se los atrapa se los envía a la arena para que los devoren los leones".*

Fue justamente uno de los participantes de este debate, Lee Felsestein, quien definió un nuevo conjunto de reglas para el hacker. Las presentó el 4 de agosto de 1989 en Amsterdam, Holanda, cuando se celebró la primera reunión internacional de hackers, la *Galactic Hacker Party*, en un centro cultural de moda, El Paradiso. La declaración propuesta por Felsestein y aprobada por unanimidad de los asistentes a la fiesta decía:

Considerando que:

La sociedad democrática esta basada en el derecho de todos a acceder a la información publica y el derecho de asociarse libremente, y que en años recientes, se han desarrollado estructuras técnicas para manipular esa información, las cuales obscurecen la accesibilidad a esa información a través de la complejidad, y que esas estructuras técnicas también sirven para aislar a la gente y para anular su derecho de asociación,

AFIRMAMOS Y DECLARAMOS:

- *El derecho a descubrir no solamente toda la información pública, sino también el funcionamiento de los mecanismos por los cuales esta información es recolectada y procesada;*
- *La responsabilidad de evitar dañar a otros mientras ejercitamos este derecho de descubrimiento, y*
- *El derecho y responsabilidad de compartir el conocimiento y las habilidades que sirven para revelar la función de los mecanismos de procesamiento de información,*

mientras guardamos estrictamente la confidencialidad de la información que ha sido confiada o entregada a dichos mecanismos por partes privadas.

- *Decimos NO a la sociedad de la información, SI a una sociedad informada.*

II. Los próceres de ayer

Put another password in Bomb it out and try again Try to get past loggin in	Ingresen otra contraseña si la rechaza, vuelvan a intentarlo. Traten de conseguir un login:
We're hacking, hacking hacking	Estamos hackeando, hackeando, hackeando.
Try his first wife's maiden name,	Prueben con el nombre de soltera de su primera esposa,
this is more than a game, it's real fun, it is the game	es mas que un juego: es verdadera diversión, es el juego.
it's hacking, hacking, hacking.	Es el hacking, hacking hacking
Sys-call, let's try a sys-call call.	Un sys-call, probemos con un sys-
Remember the great bug from version 3 Of RSX it's here WHOPPEE!	Acuérdense del gran bug que tenia la versión 3 del RSX; ¡aquí esta!
Put another sys-call in, Run those passwords out and then	Ingresen otro sys-call, agoten todas las Contraseñas y entonces
Dial backup, we're loggin in,	marquen el numero, nos estamos conectando.
We're hacking, hacking, hacking.	Estamos hackeando, hackeando, hackeando.

CRACKERS HYMNE

A mediados de los años 60 engañar a MaBell era una práctica cotidiana. Los phreakers no dejaron de acumular experiencias desde que Mark Bernay divulgó el secreto de los *loop-around-pairs* (bucles de lineas entrelazadas); la difusión de técnicas como las Blue, Black, y Red Boxes -distintos aparatitos que compartían la finalidad de hablar por teléfono evitando el disgusto de las facturas- era muy común entre los estudiantes de ingeniería. Cuando la Bell Telephone públicó la serie de doce combinaciones de seis tonos multifrecuencias que regia sus aparatos, los phreakers descubrieron que se podía controlar el sistema con un silbido de 2600 ciclos y conseguir ese sonido se convirtió en el objetivo primordial.

Joe Engressia era un niño ciego que solía entretenerse llamando asiduamente a su abuela para silbarle melodías en el teléfono. Pero, advertía con irritación, a veces la linea quedaba muda cuando él comenzaba a silbar. Por su discapacidad siempre había sentido una atracción especial por los teléfonos y el defecto lo preocupaba.

Joe tenia ocho años cuando decidió consultar a un técnico de su zona: así descubrió que su silbido alcanzaba a los 2600 ciclos, lo que provocaba el corte de linea. Joe no entendió ni jota, pero al poco tiempo dominaba por completo el sistema: también podía silbar los tonos del número telefónico al que llamaba. Después del articulo de Rosenbaum y largos meses de control, lo arrestaron y confiscaron todo su equipo.

Pasó una noche en la cárcel pero la acusación final fue por provocar daños intencionales y quedó en libertad a cambio de prometer que nunca mas haría phreaking. Para estar seguros la telefónica le quito la línea.

El Silbato del Cuáquero

Un día de 1969 el teléfono sonó en la casa de John Draper, quien por entonces tenia veintiséis años y vivía en San Jose.

- Hola, me llamo Denny y me gustaría mostrarle algo relacionado con los órganos y la telefónica - escuchó Draper en el auricular.

La frase tenía suficiente misterio como para que John viajara hasta San Francisco para ver a Denny, quién había descubierto que con un órgano Hammond producía los tonos necesarios para generar una llamada de larga distancia gratuita. El inconveniente radicaba en que debía hacer una grabación para cada teléfono con el que quisiera comunicarse, pero si conseguía un aparato que combinara los sonidos, la complicación podía evitarse. Así nació la Blue Box (caja azul), que Draper entregó a un grupo de muchachos ciegos advirtiéndoles que era ilegal. Pero era tarde: Los chicos ya militaban en el phreaking.

- Tomá, te lo regalo -dijo uno de ellos abriendo la mano que contenía el secreto.

- Que es? Un silbato? -se extraño Draper.

- Ponele una gota de pegamento en el orificio de salida y probálo. Después charlamos.

El silbato era una yapa que ofrecían las cajas de cereales Quaker Oats, identificadas con un dibujo: Captain Crunch. Cuando John probó el silbato comprendió: emitía el sonido de 2600 ciclos. Divertido, adoptó el silbato y el nombre de Crunch como su alias. Al mes siguiente, Capn' Crunch se fue de vacaciones a Inglaterra y cuando recibió la primera llamada de un amigo, usó el silbato que dió la señal de colgar a la oficina norteamericana, pero el sistema de Inglaterra no respondía a esas frecuencias y la comunicación se mantuvo. La noticia se desparramó como aceite por el mundo de los phreakers y Crunch se convirtió en el blanco de todas las llamadas. Que un turista fuera tan solicitado despertó el interés de la General Post Office (GPO, La Administración General de Correos Británica), por lo que envió investigadores a entrevistarlo aunque estos no pudieron descubrir el truco. De regreso en su país, Draper se convirtió en el rey de los phreakers: equipó una camioneta Volkswagen con una centralita, una Blue Box de alta tecnología, y recorrió las carreteras de California para utilizar los teléfonos públicos aislados. En una ocasión hizo rebotar la llamada veinte veces antes de comunicarse con un número de Roma para preguntar si estaba lloviendo. A veces escogía dos aparatos linderos para llamarse a sí mismo y escuchar su voz con el eco acumulado de una vuelta alrededor del mundo.

A raíz del articulo de Rosenbaum donde se daba cuenta de la blue boxing, Cap' Crunch fue detenido en 1972 y cuatro años después lo condenaron a dos meses de cárcel. La fama de sus conocimientos lo precedió en el camino al penal y ni bien ingresó se encontró rodeado de malandras dispuestos a tomar clases sobre el sistema.

- Bueno, pibe, bienvenido. Ahora nos vas a contar cómo es eso que haces- lo saludó uno con cara de pocos amigos en la primer oportunidad.

- ¿Para que quieren saberlo? acá no les va a servir de nada- contestó Crunch en un alarde de valentía.

- No te preocupés por lo que no te importa. Solo tenés que hablar sin preguntar.

- Si, como no. Ni lo sueñes...

Con los labios partidos, un ojo negro y algunos moretones mas, Cap' Crunch eligió al interno mas corpulento como su protector y tarde tras tarde le enseñó los métodos para engañar a MaBell. Hasta el día de hoy, Crunch sostiene que aquellos mafiosos todavía sacan provecho de sus clases. Al salir de la cárcel se integró a la People's Computer Company (PCC), cuyo objetivo era desmitificar los ordenadores y, ante el surgimiento de las máquinas personales, derivó al Homebrew Computer Club inaugurado el 5 de marzo de 1975. De allí salieron los dos Steve que fundaron Apple, para cuyas máquinas Crunch creó el Easy Writer, uno de los primeros procesadores de textos, que luego comercializó IBM con gran éxito. Lo diseñó en 1979, mientras cumplía una segunda condena por phreaking en la prisión de Pennsylvania, con la ayuda de una computadora y en las horas de su programa de rehabilitación.

Equipados

Hubo otros capitanes que comandaron las tropas en la época en que phreackers y hackers comenzaron a fusionarse. A principios de los años 70 Ian Murphy pinchaba lineas telefónicas para escuchar conversaciones ajenas y hacia del *trashing* su actividad cotidiana. Trash significa basura, y revolver en ella era una fuente de información invalorable: siempre aparecían papeles con datos jugosos (números de teléfonos, códigos, y hasta contraseñas). Con su primera computadora pasó días y noches conectándose con cuanto módem lo atendiera y hackeando todo el sistema que se cruzara en su camino. En 1979 cuando Crunch cumplia su segunda condena, ya se había convertido en Captain Zap (por un programa que evitaba la protección de softwares contra copias piratas, el Super Zap) y junto a su amigo de correrías infantiles, Doctor Diode, ingresó en el sistema de la agencia de crédito norteamericana.

- ¡Uy, uy, uy! ¡Mirá esas cuentas! Estos tipos tienen la calificación mas alta para créditos -se estremeció Diode- Están llenos de plata. Zap alzó el hombro y con un dejo de desprecio sólo murmuro:

- Nosotros también podemos estar ahí...

Sin demoras registró en los archivos del sistema una falsa corporación, solvente como ninguna. Tener una cuenta disponible sin límite de compras y no sacarle provecho es una estupidez, de modo que pensaron en darle un uso. Cuando se filtraron en el sistema de un comercio de computación tuvieron la respuesta.

- A ver, Diode... ¿Te gusta una Hewllett Packard? -preguntó Zap, mientras miraba en la pantalla la lista de productos.

- Y... podría ser. ¿Tiene impresora?

- Claro, viejo. ¿Qué pasa? ¿estás cuidando el centavo? y unos handys tampoco estarían mal, ¿no?.

Con los artículos elegidos, Zap generó la factura correspondiente, el recibo y la orden de entrega con la dirección de un correo secreto. A primera hora de la mañana siguiente, el empleado de expedición sacó de la computadora todas las órdenes de entrega y envió a cada quien su compra. Para el proveedor todo estaba en orden, descubrirían la falta de dinero recién en el momento de hacer el balance. Cap' Zap y Diode recibieron el primer pedido y de allí en mas se dedicaron a "comprar" gran cantidad de artículos de computación. Lo hicieron durante dos años y agrandaron la compañía con el ingreso de tres nuevos amigos, pero en 1981 la policía comenzó a investigar a raíz de las denuncias del comerciante y los cinco fueron detenidos. Tres de ellos se declararon culpables y colaboraron con la investigación para reducir sus penas; Zap y Diode contaron con la defensa de dos de los mejores abogados de la zona. El padre de Ian -Zap- era propietario de una compañía naviera y no le costó demasiado contratarlos.

- Ningún jurado entenderá jamas lo que hiciste y ningún jurado te condenará jamas por haber burlado a la compañía telefónica- aseguró a Cap' Zap uno de los profesionales.

El tribunal se encargó de darle la razón, y a tal punto los jueces no comprendieron de que se trataba que les impusieron una multa de mil dólares y los condenaron a dos años de libertad vigilada... ¡Por teléfono! Ian Murphy fue el primer hacker perseguido por la ley en los Estados Unidos y el caso hizo que se estudiaran nuevas leyes en cuanto a delitos informáticos, aunque recién en 1986 se votó la primera.

Las Reuniones Iniciales

Cuando MaBell instaló el sistema de llamadas en conferencia, los phreakers tomaron la costumbre de reunirse en una línea en desuso en Vancouver para conversar entre ellos. La nueva forma de aventurarse requería algo mas que un teléfono y así surgieron los Bulletin Board Systems (BBSs), una computadora conectada a un módem -aparato que traduce los impulsos digitales del ordenador en señales telefónicas y viceversa, para permitir que dos máquinas se conecten entre sí- que funciona como centro de información y canal para mensajes entre los usuarios. Es posible que el primero naciera en febrero de 1978 por idea de Ward Christensen y Randy Seuss, quienes generaron de ese modo la primer instalación que puede considerarse en red (enlazadas entre sí) de computadoras personales. Pero no fue sino hasta 1983 que los BBSs proliferaron como langostas.

La película Juegos de Guerra actuó entre los amantes de la computación como un disparador: para fines de 1984, un revelamiento en los Estados Unidos detectó aproximadamente 4000 instalaciones de ese tipo. En poco tiempo evolucionaron hasta convertirse en verdaderos bancos de datos en los que se podían encontrar desde números telefónicos hasta manuales y revistas digitales con todas las novedades y comentarios sobre el tema.

Las publicaciones especiales para phreakers comenzaron con la legendaria hoja del YIPL y no pararon hasta llegar a los hackers. La aparición del primer número de una revista impresa data de 1984 y hoy

2600 The Hackers Quartely (En alusión a los 2600 ciclos de las lineas desocupadas) es la más importante en su tipo. Su director es Eric Corley (mas conocido como Emmanuel Goldstein), phreaker enamorado de los teléfonos públicos.

Mientras tanto, al otro lado del atlántico los hackers de Inglaterra comenzaban a actuar y los pioneros no sumaban mas de una docena. Triludan, The Warrior (El guerrero) y Steve Gold, un periodista de 25 años a quien la amistad con Cap' Crunch había introducido en el phreaking, acostumbraban reunirse en un restaurante chino para intercambiar sus descubrimientos. Habían aprendido los rudimentos de la computación en el colegio, ya que el gobierno británico apostaba a los ordenadores como el futuro de la sociedad.

- Anoche entré a Prestel- anunció Triludan en voz baja y excitada.

- ¡Buenísimo! ¡Por fin! ¿Cómo te fue? - pregunto Gold.

- La verdad, fue sin querer. Ya no sabía que poner cuando me pedía la identificacion (Id) y acerté repitiendo diez veces el número 2. Y la clave, no me vas a creer, es todavía mas fácil: 1234.

Prestel era una red informativa de compras y mensajes creada por la GPO a principios de los 80 y Triludan había accedido a un sistema de prueba, el primer escalón. Insistió con las combinaciones una vez por semana hasta que encontró un ID y una password que correspondía al sysman (system manager, administrador del sistema); recién entonces pudo recorrer el sistema a gusto y modificar los datos de las pantallas y los informes.

- Mirá, acá esta el cuadro comparativo de monedas -señalo Steve una noche mientras se divertía con Prestel.

- Ahá. Podríamos tocar algo, ¿no? -preguntó Triludan sin esperar respuesta- A ver, una libra igual a... cincuenta dólares.

Fueron unas horas gloriosas para la economía inglesa, al menos en las pantallas de los usuarios de la red informativa. Esa misma noche entraron en la cuenta del correo de su alteza real el Duque de Edimburgo, el Príncipe Felipe, y dejaron un saludo cordial firmado por "S.A.R., El Hacker Real". Pero la huella que desató la investigación de Prestel fue la modificación de la primera pantalla que indicaba los pasos para continuar utilizando el sistema. Prestel utilizó monitores para controlar sus líneas y seis meses después, el 10 de abril de 1985, la policía detuvo a Steve Gold y a Robert Schifreen, rebautizado Triludan por la marca de los antihistamínicos que consumía.

Este fue el primer intento en el Reino Unido de perseguir el hacking. Ambos amigos fueron acusados de falsificación y juzgados con la advertencia del juez que intervino en el caso: "No se trata de un asesinato -manifestó- pero es un caso muy importante, que va a sentar un precedente". Los condenaron a abonar multas y costas por un total de mil quinientos dólares, pero Lord Lane, presidente del Tribunal Supremo al cual apelaron, determinó que copiar contraseñas no estaba incluido en la ley de falsificaciones vigente en Gran Bretaña y revocó la medida. Gold y Triludan admitieron el hacking pero no la falsificación y el fallo favorable resultó confuso: los hackers y phreakers dieron por sentado que lo que hacían no era delito.

En Connecticut, Estados Unidos, la historia trazaba un paralelo.

- Habla John Velmont. Quiero realizar una denuncia. Recibí el resumen de mi tarjeta de crédito y figura la compra de un artículo de electrónica que no hice.

El llamado fue atendido por la policía local, que siguió el rastro de la operación con las ordenes de entrega del vendedor hasta una casilla de correo en South Plainfield, pueblo de Nueva Jersey. A ese lugar llegaban a menudo piezas de electrónica, estéreos y equipos de detección por radar comprados a través de catálogos computarizados. El titular de la casilla era New Jersey Hack Sack y durante el arresto secuestraron de su casa diskettes que contenían manuales reservados de los satélites de American Telegraph & Telephone (AT&T) y Comsat, números de tarjetas de crédito, teléfonos secretos de altos oficiales de la secretaria de defensa y datos sobre sistemas de seguridad electrónica y del personal que los manejaba.

Hack Sack lideraba un grupo de siete adolescentes de entre trece y dieciocho años que habían adquirido equipos por valor de treinta mil dólares. El método para abusar de tarjetas de crédito ajenas no era novedoso, pero los datos sobre los satélites de comunicaciones fueron una sorpresa. El caso se difundió y dio lugar a una guerra de especulaciones: ¿Y si habían variado la posición de los satélites? ¿Que consecuencias podrían sobrevenir? Si bien AT&T y Comsat negaron cualquier intrusión en sus sistemas, la posibilidad de que unos pocos chicos intervinieran las comunicaciones alteró a la ciudadanía. La investigación estuvo a cargo de Alan Rockoff, fiscal de Middlesex, Nueva Jersey, y los adolescentes fueron acusados de asociación ilícita y robo por computadora.

La Ley del Caos

Ese mismo año en Alemania, el grupo Chaos Computer Club lanzaba su propia revista, la Die Dantenschlender (la centrifugadora de datos) y promocionaba la colección de libros Die Hackerbibel (la biblia del hacker). La banda funcionaba desde 1981 por iniciativa de Herwart Holland Moritz (Wau Holland) bajo el lema "libertad de información" y a sus miembros les gustaba definirse como "viajeros de los datos". Se habían adueñado de las computadoras de la empresa Altos de Hamburgo -que jamás se preocupó por protegerlas- convirtiéndolas en un lugar de reunión de hackers, no sólo Alemanes sino del resto del mundo. En el mismo camino de Triludan, en noviembre de 1984 hackearon Bildschirmtext (BTX), un servicio de informaciónes controlado por el Bundespost, el correo alemán. Un par de meses antes Holland y Steffen Wernery habían descubierto que era muy fácil conseguir los datos de los usuarios y cargar a sus cuentas diversos servicios.

- Btx es inexpugnable, tiene severas medidas de seguridad- aseguró entonces un directivo de Bundespost.

El desafío estaba lanzado. Los miembros del Chaos ingresaron en Btx y averiguaron las claves del banco Hamburger Sparkasse. Mediante un programa, hicieron que el banco llamara durante diez horas al club y colgara al obtener respuesta. Cuando venció el plazo la cuenta telefónica del Hamburger Sparkasse ascendía a ciento treinta y cinco mil marcos y, si bien la factura nunca se cobró, Wau y Steffen obtuvieron categoría de héroes nacionales. La noticia del hackeo a la NASA efectuado el 2 de mayo de 1987, se divulgó recién en septiembre de este año -cuando ya los habían descubierto- mediante un reportaje que publicó la revista Stern. Wau relataba como habían ingresado en el Centro de Investigaciones Espaciales de Los Álamos, California; al banco de datos de la agencia espacial Europea

EuroSpand; al Centro Europeo de Investigaciones Nucleares (CERN) con sede en Ginebra; al instituto Max Plank de física nuclear; al laboratorio de biología nuclear Heidelberg (Alemania Federal) y al organismo espacial de Japón. La NASA informó ambiguamente cuando comenzaron las consultas y aceptó que los alemanes habían ingresado en sus sistemas aunque, dijeron, "a bajos niveles".

Los miembros de Chaos, por su parte, dicen que obtuvieron las passwords de altos miembros y con ellas accedieron a proyectos secretos.

Las máquinas hackeadas eran de la Digital Equipment Corporation, que había lanzado una nueva versión de su sistema operativo VAX/VMS con novedosas funciones de seguridad, pero con un terrible agujero que permitía el ingreso no autorizado. La Digital también admitió la filtración y solucionó las fallas.

- ¿Cuantas veces ingresaron? - pregunto un periodista a Wau

- Mas de cien, desde mayo - estimo Holland

- ¿Siempre de la misma manera?

- No. Para que no nos descubrieran, hicimos un programita que modificaba algunas de las funciones del sistema operativo y nos permitía ingresar sin que nos vieran. El VMS obedece a los comandos Monitor, Show y Loginout; si el administrador los ejecuta, la pantalla muestra información, incluso quienes están conectados. Lo que hicimos fue falsificar esas tres pantallas para que no nos detectaran. Después creamos otro programa que copiaba y encriptaba las passwords; lo dejábamos funcionando un tiempo, sacábamos el archivo, lo desencriptábamos y teníamos las claves para meternos con identificaciones de legítimo usuario.

- ¿Como los descubrieron?

- El primer aviso de intrusos fue dado en agosto por Lennard Philipson, jefe del Laboratorio Europeo de Biología Molecular. Pero el mayor error lo cometió uno de los nuestros: se quedó demasiado tiempo con la clave trucha, el administrador vio que se consumían muchos recursos de su maquina y ejecutó Monitor y Show. La respuesta, por nuestro programa, fue que "nadie" estaba conectado y eso no podía ser. Ahí se dieron cuenta.

Cuando Wau y Steffen Wernery contaron cuales fueron las órdenes o comandos que les abrieron camino a través de la red para llegar a informaciones de cuidado, los conocedores de la jerga quedaron asombrados. Todos eran comunes para cualquier operador familiarizado con la costumbre -propia del ambiente- de contraer dos o mas palabras.

Con *readal* (read-all, lee todo), los hackers pudieron leer los boletines y la correspondencia personal de los usuarios de todo el sistema; *oper* (*sysop*, *op*, oper y *sysman* son formas de designar al operador o administrador principal) les permitió acceso ilimitado; con *bypass* (esquivar) rodearon las áreas generales y arribaron a la información reservada y con *syslck* (*sys*, contracción de system, sistema; *lock*, bloquear) podrían haber bloqueado -según los alemanes- la interconexión de la red, algo que la NASA nunca desmintió.

Chaos no estaba solo. También en Alemania -que no pudo sustraerse al impacto de Juegos de guerra- se habían formado hacia 1985 otros clubes de hackers: Bayrische Hackerpost (BHP) en Munich, Foebud-

Bi en Bielefeld, Suecrates-S en Stuttgart y HiCap-Ce en Celle. Y entre tanta diversidad había espacio para la confusión. Dos semanas después del articulo en *Stern*, agentes alemanes y franceses allanaron el local del Chaos y los domicilios de algunos de sus miembros en Hamburgo y Heidelberg. Investigaban una denuncia presentada por el CERN y la sede francesa de Philips, que los acusaba de haber ingresado en sus redes para espiar, borrar y modificar datos secretos. Pero se trataba de un malentendido.

VMS para la KGB que lo mira por TV

Peter Kahl tenía por entonces treinta y cinco años. Era un oscuro croupier en un casino de Hannover que ignoraba todo sobre computación; todo excepto la existencia y el accionar de los hackers. Había estado en una reunión en Hannover y allí comenzó a diseñar un plan para salir de su vida oscura: armar a un grupo de hackers que lograra información de la industria militar y defensiva del Occidente para vendérsela a la Unión Soviética.

Karl Koch había gastado la herencia de sus padres comprando estimulantes que lo ayudaban a superar la depresión pero impactaban en su cabeza; después de leer la trilogía Illuminatus!, de Robert Shea y Robert Anton Wilson, decidió que su alias seria Hagbard, convencido que las conspiraciones dominaban el mundo. Ademas de las drogas se interesaba solo en el hacking.

Cuando Karhl se le acercó en la reunión de Hannover, estaba dispuesto a ser parte de la banda de espías. Los primeros dólares -inmediatamente invertidos en LSD, cocaína y haschisch- llegaron para Hagbard fácilmente: vendió software de dominio público y programas que había copiado sin costo de los BBSs a los que tenia acceso. Pero los soviéticos conocían aquello de "el primero te lo regalan el segundo te lo venden".

- El Pentágono, la NORAD, el MIT, la NASA- calculó Peter Karhl – y también Philips France. Bueno, la lista es bastante completa. Vas a tener que moverte para conseguir los códigos.

- Pero todos esos tienen VAX y yo no los conozco- protesto Hagbard.

- Querido, si no hay datos, no hay plata. Y si no hay plata no hay drogas ni nada. No lo digo yo, lo dicen los de la KGB. ¿Un consejo? Empezá ya mismo a moverte.

Hagbard necesitaba ayuda y decidió visitar el congreso anual que organizaban los del Chaos de Hamburgo. Allí estaba Pengo, en realidad Hans Hubner, un adolescente de dieciséis años que conocía todos los defectos del VAX y con quien compartía el gusto por las drogas. Unas pocas palabras alcanzaron para integrarlo a la sociedad aportando un programa -cedido por Steffen Weihruch, renombrado como "el genio de las VAX" y asiduo asistente a las reuniones del Chaos -que capturaba login y contraseñas de los sistemas operativos VMS que usaban las VAX.

- Hagbard, muchacho, del otro lado de la cortina quieren datos sobre UNIX -solicitó Kahl al poco tiempo.

- ¿Qué? ¿Nunca se van a conformar? -se quejó Hagbard -.No tengo idea de cómo es eso.

UNIX es un sistema operativo que funciona en casi todas las computadoras y por entonces estaba en auge, aún para las VAX. Hagbard no tuvo mas remedio que concurrir a las reuniones del Chaos y esta vez la providencia lo acercó a Marcus Hess, empleado de una empresa especialista en UNIX. Tan

adicto a los coches deportivos como Hagbard y Pengo a ciertas sustancias químicas, Marcus no opuso demasiada resistencia y pasó a formar parte del grupo. Con su incorporación y los datos que brindo, los espías ganaron dos mil quinientos dólares, toda una fortuna para esa banda de marginales.

Mientras Hagbard y compañía hackeaban para la KGB, Bach y Handel, dos adolescentes identificados como VAXbusters (caza-VAX), descubrieron tres máquinas de ese tipo en red instaladas por SCICON, una de las compañías de software mas importantes de Alemania. Cuando intentaron entrar teclearon lo primero que se les ocurrió ante el pedido de identificación y un mensaje de "error" apareció en la pantalla.

- Dale Enter- sugirió Bach -quizás nos deja intentar de nuevo.

- Ok. ¡¿qué?!- exclamo Handel -¡nos dió paso, mirá! Ahora nos pide la contraseña.

- ¡Dale enter otra vez! Es un bug, seguro.

Bach tenía razon. La máquina tenia un error de configuración, bug (insecto, bicho) en la jerga. Los VAXbusters estaban dentro del sistema. Steffen Weihruch, espías y adolescentes eran demasiadas manos en un plato y las investigaciones comenzaron.

La primera pista surgió en 1986 en los laboratorios de investigación espacial de Lawrence Berkeley, California. Clifford Stoll, astrónomo empleado de los laboratorios, denunció que personas no autorizadas habían intentado obtener datos con códigos tales como nuclear, ICBM, Starwars o SDI. En 1987 Roy Omond, director de un sistema VAX en Heidelberg, descubrió los verdaderos nombres de los VAXbusters y los publicó en un mensaje al resto de los usuarios de la red europea SPAN. Cuando Bach y Handel se vieron descubiertos les ganó el miedo y recurrieron al consejo de los miembros del Chaos, de quienes eran amigos. Por intermedio de un tercero, los hackers profesionales consiguieron que los servicios secretos alemanes -en conjunción con los técnicos de la Digital Equipment- acordaran una entrevista con los chicos bajo promesa de no tomar represalias legales.

Los VAXbusters prepararon un informe minucioso con todas las cerraduras que estaban en su poder: habían entrado en diecinueve centros de la NASA a través de SPAN, entre los que Philips no figuraba. Ya en la reunión demostraron ante cámaras como lo hacían e instalaron un "parche" para arreglar el bache en la seguridad. El video se difundió por la televisión y la investigación quedo prácticamente cerrada. Pero Philips de Francia estaba dispuesta a perseguirlos (también a los del Chaos), convencida que eran los responsables del espionaje en la empresa. En SECURICOM, feria internacional de seguridad en comunicaciones que se realiza en Francia, detuvieron a Steffen Wernery, quien se había ofrecido para conferenciar, y lo mantuvieron encarcelado tres meses, tiempo que demoraron las autoridades francesas en aceptar su declaración de inocencia.

La confusion de Phillips era conprensible. Tanto los VAXbusters como Weihruch y el grupo de espías usaban las mismas técnicas para hackear, en tanto Wernery solo había sido mediador y cara visible en las explicaciones televisadas después de la conmoción que causo el caso de Bach y Handel.

Mientras Wernery sufría cárcel en Francia, los responsables del espionaje seguían en Alemania, sanos y salvos de la legislación francesa pero preocupados por los allanamientos y arrestos de miembros del Chaos y por la creciente presión de la KGB, que se endurecía en los pedidos y plazos.

En el verano de 1988, Pengo y Hagbarg pensaron sacar provecho de una amnistía en la ley de espionaje para aquellos que colaboraran con los investigadores y no registraran antecedentes. Amparados en ella se declararon espías y fueron testigos de cargo en el juicio contra Hess y Kahl. Alexander Prechtel, portavoz de la fiscalía federal alemana, confirmó a través de la cadena de radio y TV NDR "el desmantelamiento de la red" y anuncio la "detención de tres de sus miembros que operaban en la RFA y eran coordinados por dos agentes de la KGB". Hess fue condenado a veinte meses de prisión y una multa de diez mil marcos; Kahl a dos años y tres mil marcos, pero ambas sentencias se sustituyeron por libertad condicional. Dos meses después del juicio el cuerpo de Hagbard apareció carbonizado. El hecho nunca pudo aclararse y fue cerrado como suicidio.

Padres e Hijos

El 2 de noviembre de 1988 se cumplieron cinco años desde que Fred Cohen declaró oficialmente el nacimiento de los virus informáticos. Como Cristobal Colón y el descubrimiento de América, Cohen fue el primero en declararlos aunque no el primero en hacerlos, pero esa es otra historia.

Ese día, en el laboratorio de Inteligencia artificial del MIT, las computadoras SUN con sistema operativo UNIX conectadas a Internet (red de redes mundial) empezaron a comportarse de una manera extraña. La máquina VAX de la Free Software Foundation, cuya dirección en la red era prep.ai.mit.edu, también tenia problemas.

- Peter, ¿que le pasa a las maquinas? -pregunto Mark, su compañero.

- Mmm... No sé... No entiendo... Parece que hay algún proceso ejecutándose -contestó Peter-, un proceso que consume muchos recursos... El promedio de uso era 5 la última vez que miré. Ahora es de... ¡7.2!

- Imposible. A esta hora no puede ser mas de 2. Mirá de nuevo.

- Ahora está en 8... Hay unos treinta procesos en ejecución, pero no veo nada anormal en ellos excepto que si trato de matarlos aparecen de nuevo.

- Bueno, vamos a tener que resetear- propuso Mark mientras tipeaba los comandos necesarios para volver a arrancar la máquina. Minutos después la computadora funcionaba normalmente. Pero no duró mucho.

- Mark -llamo Peter-, te tengo malas noticias... ¡Empezó todo de nuevo!

- Creo que tenemos un problema grave. Ambos eran operadores de la red de Rand Corporation de Santa Mónica, a miles de kilómetros del MIT, y a las 20 horas de aquel día detectaron la primera señal de anormalidad en las computadoras. A las 22:30 los administradores del sistema de la Universidad de California, en Berkeley, pensaron que un hacker los atacaba.

- Detectamos un virus en el Laboratorio de Medios -escribió en el correo electrónico a la 1:10 de la madrugada, Pascal Chenais, del MIT-; sospechamos que toda la red Internet esta infectada. El virus se propaga a través del correo, por tanto no aceptaremos ni enviaremos mensajes.

- Nos ataca un virus de Internet. Ya contagió la Universidad de San Diego, Livermore, Standford y Ames -indicaba un mensaje de Peter Yee, del Laboratorio Ames de la NASA, a las 2:28.

Durante esa madrugada el Laboratorio de Investigacion Balística de Maryland se desconectó de la red y permaneció aislado una semana. No fue el único: tantos centros clausuraron sus conexiones que el correo electrónico quedo bloqueado. A las 3:34 un mensaje anónimo desde Harvard explicaba cuales eran los tres pasos necesarios para detener ese misterioso virus. Pero era tarde: el caos se había instalado en la red y nadie quería estar conectado. Los lugares afectados indicaban que todo había comenzado en ARPANet, de donde saltó a MILNet y de allí a Internet, que enlazaba por sí sola a más de cuatrocientas redes locales.

Los equipos de técnicos pensaron que las sesenta mil computadoras conectadas por medio de las redes corrían peligro, pero cuando comenzaron a investigar descubrieron que el virus solo atacaba a dos modelos de maquinas: las Sun 3, de Sun Microsystems, y VAX, de Digital Equipment, que trabajaban con sistemas operativos UNIX, de la variante BSD. También determinaron que no era un virus sino un programa que se reproducía hasta embotar los sistemas y no afectaba los datos. El programa era un hacker automático. Explotaba bugs y fallas de seguridad en tres programas estándar en Internet y seguía una técnica para adivinar contraseñas y usar las cuentas de los usuarios legítimos, e infectar cuentas en otros sistemas. Los medios de prensa dijeron que era la obra de un genio, pero el experto Eugene Spafford, de Purdue University, señaló en su análisis de los hechos: "Una conclusión que puede sorprender a algunas personas es que la calidad del código es pobre, incluso se la puede considerar mediocre. No podemos discutir que el programa funcionaba. En efecto -agregó-, todos deseamos que hubiese sido menos capaz. De todas formas tuvimos suerte, porque el programa tenía errores que evitaron que funcionara a toda su capacidad".

El incidente no fue una sorpresa para los expertos que, si bien no esperaban un ataque de este tipo, sabían que algo así podía suceder y conocían las fallas de seguridad del UNIX: los mecanismos para detectar las contraseñas de los usuarios eran demasiado populares.

Un paper sobre el asunto fue publicado por Robert Morris y Ken Thompson en 1979, pero muy poca gente se preocupó seriamente por aplicar los datos que recogieron los dos investigadores. En su época de hacker, Robert Morris, junto con Thompson y otros, desarrolló el juego Core War, una lucha de dos programas en el área de memoria de una computadora hasta borrar las defensas del oponente, prohibido en la universidad por ser un peligro para la seguridad del sistema. En 1988 Morris trabajaba en el Centro Nacional de Seguridad Informática y tenia un hijo de veintitrés años, Robert Morris Jr., no sólo conocedor del UNIX sino también lector de los textos de su padre, incluyendo el "UNIX Operating System Security", que contenía esta frase: "Hay una fina línea que divide el hecho de ayudar a los administradores a proteger sus sistemas y el darles una receta a los chicos malos". Cuando escribió eso, en colaboración con F.T. Grampp, en 1984, Morris nunca imaginó que uno de esos chicos malos iba a ser Junior, quien usó la terminal de su padre para aplicar lo aprendido en el programa que cambió la historia de Internet.

Mientras las telefónicas peleaban con los phreakers, los científicos fundaban Internet: la primera idea surgió de la Agencia de Investigaciones de Proyectos Avanzados del Departamento de Defensa. Al comienzo solo los investigadores tenían acceso a la red y la mera palabra de caballero les garantizaba que nadie leería sus mensajes. Pero el programa de Robert Morris Jr. provocó que la población de Internet se dividiera en dos: los que sabían y los que no. Los primeros comprendían la jerga, qué había sucedido y cómo; los segundos no entendían nada y se preguntaban qué significaba tal palabra, o cómo

hacer tal cosa. Desde entonces, la seguridad en Internet no pudo sino empeorar, a punto tal que en Holanda algunos profesores de computación asignaron a los estudiantes un sitio en la red para quebrar, entrar y sacar archivos como prueba práctica de que comprendían el protocolo.

El espíritu de investigación que caracterizo a los hackers, y su necesidad de encontrar nuevas puertas, los llevo a inventar programas que sirvieran para diversas funciones. Era casi inevitable que en algún momento se preguntaran que podría pasar con un programa que se reproduce a si mismo.

Uno de estos testeos -origen de los virus- dio nacimiento a los "gusanos", un programa que reside en la memoria de las computadoras y se reproduce pero en máquinas conectadas con la primera. Cuando un gusano se activa ocupa espacio vital de la memoria y el ordenador se vuelve mas lento. No necesita ningún elemento para anexarse, ni archivo ni programa. El virus Internet correspondía a este tipo.

- Nunca tuve intención de estropear las computadoras o provocar que funcionaran mas lento -se disculpó Robert Morris Jr. Introdujo el gusano en la Internet por la simple curiosidad de ver que sucedía; no supo calcular la velocidad de la reproducción y para cuando envió el mensaje anónimo a través de su amigo de Harvard, Andrew Sudduth, ya era tarde.

Lo juzgaron conforme a la Ley de Fraudes y Abusos Informáticos estadounidense por "Acceder intencionalmente y sin permiso a ordenadores de interés federal" y en 1990 el juez Honard Munson lo condenó a tres años de libertad condicional, multa de diez mil dólares y cuatrocientas horas de servicio comunitario.

Sale con Fry

En 1989 Fry Guy tenía quince años. Necesitaba dinero. Después de dos años de dedicarse al phreaking y hablar con la otra mitad del mundo, los gastos de su cuenta telefónica aumentaron del mismo modo que sus problemas familiares. Encontró la solución en la CSA (Agencia de Crédito), pero le faltaban algunos datos.

- Operadora, soy Mike Wilson de apoyo técnico. Necesito que saque una ficha reservada. Tipee...

Fry Guy continuó con las órdenes disimulando la voz para parecer mayor y la operadora obedeció. Aplicaba una técnica muy difundida -la ingeniería social- para obtener información valiosa engañando al interlocutor. Con el mismo método convenció a un comerciante de que era un empleado de la CSA y obtuvo los códigos de acceso del comercio, con los que ingresó en la agencia. Una vez conectado, eligió en la lista de clientes a Max Adams, comprobó que era solvente, anotó el numero de teléfono y se desconectó.

Llamó a la telefónica, manipuló los *switches* y redirigió las llamadas de esa persona a su casa. Marcó otro numero.

- Western Union, ¿en que puedo ayudarlo? -escuchó Guy.

- Habla Max Adams -dijo con aplomo-, quiero hacer una transferencia de efectivo de mi cuenta.

- Cómo no, señor Adams. ¿Cuánto y adónde quiere transferir?

El dinero fue enviado a una sucursal a la orden de un amigo del hacker, que esperó la llamada de confirmación y luego devolvió las lineas a su orden. Al día siguiente retiró el dinero, pagó sus deudas y disfrutó del resto.

Ese verano repitió la operación varias veces. Fry Guy obtuvo los datos necesarios para hackear en el BBS Atlantic Alliance y se especializó en el sistema telefónico; se introducía en el ordenador que controlaba todos los números y les asignaba distintas funciones o los redireccionaba. Llegó a conocer de tal modo a la telefónica Bell South de Atlanta que los demás hackers lo reconocieron como su SoI, Sphere of Influence, esfera de influencia. No siempre acaparaba su botín, en una oportunidad accedió a través del Sprint Telenet System a la red de la cadena McDonald's; con los privilegios de supervisor, alteró los registros y logró que la empresa otorgara generosos aumentos a sus amigos que trabajaban friendo papas.

Fiesta Hacker

En 1988 el Paradiso, un importante centro cultural de Ámsterdam, organizó una conferencia con los mas famosos hackers alemanes del *Chaos Computer Club* y hasta allí llegó en procesión un grupo de hackers holandeses, el *Hack-Tic*, que presentó entre los asistentes uno de los primeros números de su revista. El éxito de la reunión motorizó la intención de repetir el evento a mayor nivel: con mas gente, mas días, mas tecnología y con hackers de toda Europa. Holanda era el lugar ideal para organizarlo: en ese momento no tenía leyes contra el hacking. La idea siguió dando vueltas. Para la Navidad del 88' Caroline Nevejan, del Paradiso, Patrice Riemens, un amigo de ella, y Rop Gonggrijp, director y líder informal de Hack-Tic, asistieron al Chaos Communications Congress, que se realiza todos los años en Hamburgo para esa fecha. Ahí, entre hackers y redes, terminó de cristalizarse la súper reunión a realizarse en el Paradiso en agosto del año siguiente: Rop sería el representante del movimiento hacker, Caroline trabajaría en el Paradiso y Patrice se ocuparía de la papelería. Necesitaban un nombre para identificarlo y optaron por Galactic Hacker Party, un juego de palabras relacionado con la serie de novelas de Douglas Adams, Guía del autoestopista galáctico.

Su primer acuerdo fue mostrar el hacking como un movimiento social para cambiar la imagen que el público y los medios tenían del fenómeno. Pusieron mucho cuidado en hacer la lista de invitados internacionales: uno era Lee Felsestein, parte fundamental del proyecto Community Memory, en Berkeley -donde intentaban acercar las computadoras a la gente común, brindándoles una herramienta de poder- y cofundador del Homebrew Computer Club. Su presencia fue decisiva, al punto que propuso la declaración de principios que cerró el congreso. También estaba Cap' Crunch, quien fue el encargado de abrir los intercambios con otros países, haciendo gala de sus habilidades. En representacion del Chaos Computer Club asistieron Hans Hubner (Pengo), Steffen Wernery y Wau Holland. La revista 2600 participo desde los Estados Unidos, y hackers de otros países estuvieron presentes intermediados por las redes de datos.

El titulo "formal" de la Galactic Hacker Party fue ICATA '89, International Conference on the Alternative use of Technology in Amsterdam (Conferencia Internacional sobre el Uso Alternativo de la Tecnología, en Ámsterdam). El programa de actividades contempló debates sobre:

- "To Byte or Not to Byte" (juego intraducible con "To Be or Not to Be"), dedicado a la relacion entre el hombre y la maquina, la inteligencia artificial, la creatividad y las computadoras, la democracia por computadora, las consecuencias de los virus y la relación de los ordenadores con la tecnologia.
- "The Hacker in the Lion's Den" ("El hacker en la guarida del leon"), en el que se habló de las relaciones entre las grandes empresas, los gobiernos y sus servicios secretos y el derecho a la información, la legislación sobre el hacking y la censura en las redes.
- "The Future Behind The Computer" ("El futuro detrás de la computadora"), que trató sobre el libre flujo de la información, en especial desde el punto de vista del Tercer Mundo.

La apertura se realizó mediante una pantalla gigante con la imagen del personaje televisivo Max Headroom que decía: "S-s-s-simplemente corran hasta la computadora mas próxima y hackeen t-t-t-tanto c-c-como puedan. Creo que me estoy ye-y-yendo de línea ahora". La pantalla quedó en blanco y en medio de gritos y carcajadas, los asistentes hicieron lo que Max pedía. Pero no sólo hackearon, también hablaron para ellos y para los que estaban afuera. Cap' Crunch se ocupó de criticar al gobierno del Reino Unido, volcado al estudio de nuevas leyes para castigar el hacking con hasta diez años de prisión. "Durante mi condena en los Estados Unidos -relato- fui obligado a enseñar a distribuidores de drogas y otros criminales como pinchar un teléfono, por eso ahora advierto que estipular que el hacking sea una ofensa criminal podría llevar a que se creen en prisión escuelas de hacking ilegales". Los gobernantes británicos hicieron oídos sordos al mensaje.

Durante la conferencia sobre hacking y ética Wau Holland se dirigió con dureza a Pengo. "La información debería ser libre -aseguro-, pero no para proporcionarla a la gente equivocada. Tenemos la obligación de ser responsables. Esto lo discutimos en el Chaos y nuestra conclusión es que si se hackea una planta nuclear se puede provocar una catástrofe, de modo que la responsabilidad es enorme. Con tu comportamiento, Pengo, destruiste la confianza personal". El chico reconoció estar arrepentido, pero agrego:

"No puedo cambiar el pasado. Nadie se cuestiona su ética cuando está hackeando y, por otra parte, la gente del Servicio Secreto no está interesada en cuestiones éticas". Holland le advirtió: "Desde ahora sos parte del juego de los Servicios Secretos. Sos su prisionero porque cruzaste un límite que no debías". Pero no todos los asistentes compartían ese punto de vista. Mientras se llevaba a cabo el debate, otros integrantes del congreso hackeaban el sistema telefónico holandés y el propio sistema de encuentro. ¿Que otra cosa podía esperarse de una conferencia de hackers?

Durante la fiesta, los hackers europeos descubrieron que en algunos países del Tercer Mundo tenían colegas con actividades mucho más serias que las de sus vecinos. Mientras en los Estados Unidos y Europa hackers y policías jugaban al gato y al ratón con livianas consecuencias -como cárcel por un tiempo o confiscación de equipos-, en el Tercer Mundo las computadoras se usaban para que algunas organizaciones de derechos humanos mantuvieran contacto con otros países. En Malasia, por ejemplo, era común que la policía rompiera los equipos y golpeara a la gente si un grupo on-line no resultaba del agrado del gobierno. El mensaje a los hackers del Norte era claro: ustedes juegan, nosotros trabajamos. No cayó en saco roto.

La conferencia llevó a que los holandeses desarrollaran proyectos como Digital City -un sistema on-line conectado a Internet con información para los habitantes de Amsterdam-, o la Fundación HackTic que provee acceso a Internet a precios populares. El intento de presentar a los hackers como guías para el consumidor en la era de las computadoras fue todo un éxito, y el congreso se convirtió en una leyenda.

Después de la fiesta, el movimiento hacker holandés multiplicó su difusión, la revista *Hack-Tic* fue muy requerida y sus miembros una referencia obligada para la prensa cada vez que se presentaba una noticia involucrando computadoras. Un día, sin previo aviso, las tarjetas de identidad de los estudiantes holandeses -que les permiten el acceso a los medios públicos de transporte- fueron renovadas por otras que contenían una antena en forma de chip. Cuando los medios consultaron a Hac-Tic, la revista aclaró que su circuito servia para "detectar las tarjetas en ciertos lugares; puede ser usado para contar los estudiantes que pasan por las estaciones de tren, por ejemplo, lo que significa una violación a la privacidad". Los ferrocarriles se encontraron con un serio problema de relaciones públicas tratando de explicar la situación.

A medida que el tiempo pasaba, Hack-Tic se afianzaba como un movimiento que trascendía a la revista, su actividad principal. En 1992 decidieron crear la Fundacion Hack-Tic, que brindaba servicios de Internet al público. En principio se llamaban hacktic.nl, pero hubo quienes se opusieron a la palabra hack en el nombre, ya que no querían ser asociados con hackers, y cambiaron la denominación a xs4all (Access For All, Acceso para todos). En 1994 Patrice Riemens, durante su visita a Buenos Aires, comento que "el gobierno de Holanda tiene una larga tradición de tolerancia hacia los hackers. Ellos quieren ser eficientes y reconocieron desde hace mucho tiempo que la represión cuesta dinero; perseguir a quienes no son realmente peligrosos es también una pérdida de dinero. Hasta la policía tiene una cuenta en xs4all y nadie se asombra por eso".

III. Nuevas estrellas

"Le pregunté a uno de ellos por qué habían elegido un nombre tan amenazante. "A nadie le gustaría una mariconada del tipo Liga de Recolectores de Flores". Pero los medios de comunicación también lo confundieron. Trataron de probar que la League of Doom (Liga de la Muerte) era una especie de banda, o algo por el estilo, cuando en realidad se trataba de un montón de tarados detrás de una terminal de computadora'."

JOHN PERRY BARLOW EN CRIME AND PUZZLEMENT (CRIMEN Y CONFUSION)

El Chaos Computer Club entró en la NASA, miraron los archivos durante seis meses antes de que los descubrieran y -como si fuera poco- lo anunciaron públicamente. Otros alemanes vendían información confidencial a la KGB y también lo reconocían sin que intervinieran los servicios norteamericanos. Unos holandeses atrevidos organizaban un Congreso Internacional de Hackers y nadie reaccionaba en contra. Los seiscientos millones de tarjetas de crédito que circulaban en los Estados Unidos, los cuatrocientos mil millones de dólares que el sistema de computación interbancario en red telefónica manejaba por día, los archivos con datos de clientes, transacciones y planes de negocios de compañías y bancos corrían riesgo permanente. Las bases militares eran reiteradamente hackeadas: la de las Montañas Rocosas guardaba centenares de misiles nucleares teleguiados, la Strategic Air Command, en Colorado, era el cerebro de la flota de bombarderos nucleares. Todas estas actividades se manejan por computación, por lo que la debilidad del sistema constituía un gran peligro. Los servicios secretos norteamericanos comenzaron a tomar cartas en las investigaciones.

En el diseño estratégico del plan policial, el primer paso fue el control de los centros donde los hackers encontraban siempre alguna información: los BBSs.

- Pienso iniciar una investigación personal sobre los hackers que vendieron información a los rusos. ¿Quieren unirseme en esta cruzada contra esos mierdas que manchan nuestra imagen? -invitó Skinny Puppy a través de un mensaje en el BBS Black Ice, favorito de la banda League of Doom (LoD), dos dias después del arresto de Hagbard, Pengo y compañía.

- Cuidado -respondió The Prophet-, vas a llamar la atención de las autoridades. Los federales se nos van a acercar.

- Penetremos en las computadoras soviéticas -terció The Highwayman- y entreguemos la información que haya a la CIA.

- Pero si este gobierno merece que lo jodan -consideró The Urvile-. A la mierda Norteamérica...

El Servicio Secreto tomó nota de cuanto comentario paso por el correo del BBS y la teoría de la conspiración comunista encontró buenos puntos de apoyo para salir a flote. La LoD era a los Estados Unidos como el Chaos a Alemania. Surgió en 1984 por iniciativa de Lex Luthor, quien instaló uno de

los primeros BBSs para hackers, considerado como punto de reunión de la élite: ingresar en él no era sinónimo de ser miembro de la banda.

Hacia 1989 los integrantes de Black Ice estaban metidos de lleno en una dura guerra por el dominio del ambiente con otras dos bandas, la DPAC (manejada por Sharp, Remob, GZ y Supernigger) y la Masters of Destruction (MoD, que contaba entre sus miembros a Corrupt, Renegade y The Wing). La pelea se libraba a través de las lineas telefónicas, con mensajes y amenazas en BBSs o contestadores telefónicos. Los agentes miraban y avanzaban.

Hackeado el 4 de Julio

- Hola. Hay cinco bombas de tiempo informáticas diseminadas en tus sistemas 5ESS, en distintos lugares del país -escuchó por el auricular Robert S., director de seguridad de Indiana Bell Telephone-. Van a detonar en un feriado nacional. El juego consiste en encontrarlas antes de que se ejecuten.

- ¿Cómo? Pero... ¿Hola? ¡Hola, hola! ¡Desgraciado!

La comunicación se había cortado. Era el 29 de junio de 1989 y en cinco días se festejaba la Independencia de los Estados Unidos. Robert estaba acostumbrado a recibir llamadas de los hackers, pero ninguna había sonado tan amenazadora como esa. Una bomba es un programa corto: podía estar escondida entre miles de órdenes de cualquier conmutador 5ESS. Si se ejecutaba podía generar una catástrofe: un gusano que se reprodujera y atiborrara las lineas, recargara el sistema o dejara un conmutador en un bucle sin salida. El 5ESS era un nuevo software que manejaba los sistemas de conmutación electrónica y la telefónica lo había instalado en el ochenta por ciento de sus oficinas; si entraban en bucle no pasarían llamadas sino que estas girarían dentro del conmutador interminablemente, como la púa de un tocadiscos cuando cae en un surco defectuoso.

Robert informó de la llamada a la Bellcore (Investigacion de Comunicaciones de la empresa) y desde allí se dio aviso al Servicio Secreto, responsable desde 1984 de delitos informáticos luego de una larga pelea con el FBI. Con el nuevo dato la investigación se adelantó. Ya estaban al tanto del proyecto Phoenix, anunciado en la revista electrónica PHRAC, que proponía "un nuevo comienzo de la comunidad de hackers y phreakers, en el que el conocimiento es la clave del futuro. Las industrias de las telecomunicaciones y la seguridad no pueden coartar el derecho de aprender, explorar o poseer conocimientos". Para los agentes era una proclama siniestra: ¿derecho de explorar y aprender? ¿De donde habían sacado eso?

- Bueno, Dictator -comenzo el investigador con tono irónico-, nos caíste del cielo. ¿Sabés cual es la pena que te corresponde, no? El muchacho negó con la cabeza atemorizado. Era el operador de Dark Side, BBS ilegal que funcionaba en Phoenix, Arizona. Aunque hacía varios años que se dedicaba al hacking no tenía mucha experiencia con la policía.

- Mirá, te vamos a proponer algo -continuó el agente- que te conviene aceptar. No tenés antecedentes y te haría muy mal empezar a acumularlos ahora, al por mayor.

- ¿De qué se trata?- quiso saber, nervioso, The Dictator.

- Como necesitamos algunos datos vamos a dejar que tu BBS siga funcionando, pero para que cooperes con nosotros.

Con un Bulletin Board como base, los servicios secretos controlaron los avances del proyecto Phoenix y organizaron la mayor redada de hackers en los Estados Unidos: la operación Sundevil, nombre copiado del de la mascota de la Universidad de Arizona.

El tercer día de julio, los técnicos de Bellcore localizaron tres bombas en Georgia, Colorado y Nueva Jersey. La amenaza no había sido una fanfarronada y el peligro de que las otras dos estallaran antes de ser descubiertas logró que el tribunal de la ciudad autorizara la grabación de las comunicaciones de The Prophet, The Urvile y The Leftist, integrantes de la LoD. The Prophet habia estado preso seis meses durante 1986 por "acceso sin autorización a una red computacional" (la de datos de Southem Bell) en Carolina del Norte; su condena establecía, ademas, ciento veinte horas de trabajo comunitario y tres años de control. Con las cintas como prueba, el 21 de julio de 1989 allanaron los domicilios de los tres y encontraron gran cantidad de manuales sobre la telefónica, diskettes, computadoras y miles de anotaciones.

- Ajá, hubiéramos podido interrumpir el servicio telefónico -admitia The Leftist, relajado, durante el interrogatorio.

- ¿Colocaron las bombas?- pregunto el oficial.

- ¡Por favor...! Claro que no.

Entre los papeles incautados por los servicios secretos, el documento E911 describía el programa mejorado del servicio de emergencias al cual los ciudadanos acudían para llamar a los bomberos y la policía o pedir ambulancias. "Que los hackers tengan esa información -coincidieron los técnicos de Bellcore- es terriblemente riesgoso." Las bombas eran un juego de niños comparado con eso.

Ese mismo día, pero en la localidad de Indiana, se realizaba, tras una larga búsqueda, otro arresto: el de Fry Guy. Un mes antes Fry había derivado las llamadas dirigidas a una oficina local de Florida hacia una de informaciónes de larga distancia y al día siguiente desvió las que se dirigían a la oficina de libertad vigilada de Delray Beach hacia un servicio Erótico de Nueva York, Dial-a-Porno. Fue suficiente para que los técnicos de Bell South controlaran las comunicaciones, detectaran el número y pasaran el dato a Bellcore, donde se dispusieron a escuchar todas las llamadas; así descubrieron que Fry Guy se conectaba con la CSA y se enviaba dinero a Kentucky con un numero de tarjeta de crédito. Cuando estos datos llegaron a los agentes del servicio secreto, lo incluyeron e la lista de sospechosos -sobre todo porque vivía en la misma ciudad donde se había realizado la llamada amenazadora de las bombas informáticas- y el 29 de julio allanaron su casa.

Crimen y Confusión

A las 2:25 de la tarde del 15 de enero de 1990 todas las llamadas de larga distancia, nacionales e internacionales, de la red AT&T -la compañía telefónica mas importante de los Estados Unidos- comenzaron a recibir la misma respuesta: "Todos los servicios están ocupados; por favor, intente mas tarde", repetía la grabación de una voz femenina. Durante ese día, veinte millones de llamados no llegaron a destino y mas de la mitad del país quedo incomunicada. Durante la tarde y hasta la madrugada, los técnicos tuvieron que reemplazar el software de las centrales de conmutación telefónica de la mitad del país para solucionar el problema. Robert Allen, presidente de AT&T, sostuvo al día siguiente que el problema había sido una falla en el software UNIX, pero otros voceros aseguraron que

se trataba de un ataque de hackers. Con los antecedentes de arrestos e intromisiones recientes, el público norteamericano decantó hacia la teoría del hacking y exigió que se castigara a los culpables.

El 19 de enero los servicios secretos arrestaron a Knight Lighting, coeditor de *PHRAC* y operador del BBS Metal Shop -en realidad Craig Neidorf, estudiante de veinte años-, por haber publicado el 25 de febrero de 1989 el documento E911 en su revista electrónica. El 24 detuvieron a Acid Phreak -Joey-, sospechoso de ser el responsable de las bombas informáticas descubiertas por los hombres de Bellcore. Un día después allanaron el domicilio de Phiber Optic -Mark Abene-, miembro de LoD desde hacia un año, y el de The Mentor (Loyd Blankenship), operador del BBS trucho Proyecto Phoenix y empleado de una compañía que vendía juegos de computadora; Steve Jackson Games. Horas mas tarde se trasladaron hasta esas oficinas y, ante el asombro del propietario -el mismísimo Steve Jackson-, secuestraron todos los equipos de computacion, diskettes y papeles.

Buscaban un manual escrito por The Mentor -argumentaron- sobre delitos informáticos, que estaba en preparación para ser editado. El 8 de mayo mas de ciento cincuenta agentes del servicio secreto, en colaboración con fuerzas policiales locales, efectuaron veintisiete registros en Chicago, Cincinnati, Miami, Los Angeles, Nueva York y Phoenix, entre otras ciudades, y confiscaron cuarenta computadoras y veintitrés mil diskettes.

Los cargos que se levantaron fueron tráfico y abuso de tarjetas de crédito y de códigos DDI, acceso no autorizado a computadoras y fraude en telecomunicaciones.

- ¿Mitch? Habla John. ¿Leíste las noticias sobre la redada de hackers de hace una semana?- preguntó Barlow, letrista de la banda Grateful Dead.

- Si, claro. Todo el mundo habla de eso. ¿Por qué?- contestó Kapor, coautor del exitoso programa de planillas de cálculo Lotus 1-2-3.

- Estuve pensando en las averiguaciones que hizo ese agente de la FBI entre los miembros de la red WELL y es obvio que no entienden nada de lo que es el hacking. Me preocupa mucho. ¿Porque no venís hasta casa y lo charlamos?.

- Okay. ¿Que tal mañana? John Perry Barlow y Mitch Kapor se encontraron.

Apenas días antes, ellos -entre otros- habían recibido la visita de un agente del FBI que investigaba el paradero de Cap' Crunch, a quien creían relacionado con los soviéticos y con una empresa que tenía grandes contratos secretos con el gobierno sobre la Guerra de las Galaxias. Ninguna de esas especulaciones era acertada, pero la ignorancia de los federales y la eterna teoría de la conspiración comunista preocupo a ambos. Mediante Whole Earth 'Lectronic Link (WELL, Enlace Electrónico de la Tierra), el BBS de la Point Foundation -semilla de la Conferencia de los Hackers, que se realizaba anualmente-, recibieron las protestas indignadas de otros usuarios que también habían sufrido las visitas del FBI y que habían escuchado la misma historia.

- Ese tipo no distingue un chip de un torno- desprecio Barrow-; si todos son así, quien sabe de que culpan a los hackers que detuvieron hace una semana.

- Hummm... -aceptó Mitch-, esos chicos necesitan ayuda.

En dos horas se organizaron y escribieron el manifiesto "Crime and Puzzlement" (Crimen y confusión) que anunciaba la voluntad de crear la Electronic Frontier Foundation (EFF), organización política destinada a "obtener fondos para la educación, el hobbing y los litigios en las áreas relacionadas con el discurso digital y la extensión de la Constitución al ciberespacio". El documento también declaraba que la fundación "conducirá y dará su apoyo a los esfuerzos legales por demostrar que el servicio secreto ejecutó restricciones previas a las publicaciones, limitó la libertad de expresión, tomó en forma inapropiada equipos y datos, usó la fuerza y, en general, se condujo de un modo arbitrario, opresor y anticonstitucional". Los fundadores recibieron el apoyo económico de muchos tecnócratas de la industria, incluidos Steve Wozniak, padre de Apple (que donó ciento cincuenta mil dólares), John Gilmore, uno de los pioneros de Sun Microsystemms, y Steward Brand, de la Point Foundation. El 10 de julio de 1990 la Fundación estaba en regla y se hizo cargo del primer caso: el juicio a Craig Neidorf, que comenzó el 23 del mismo mes.

Neidorf fue procesado por fraude, abuso y transporte interestatal de propiedad privada, cargos centrados en el documento E911. Cuando lo arrestaron, y tras cuatro horas de interrogatorio, Neidorf admitió que The Prophet le había entregado el documento E911 robado mediante hacking, a pesar de lo cual se declaro inocente. No fue el caso de The Urvile, Leftist y Prophet, quienes se declararon culpables y estuvieron dispuestos a cooperar para mitigar sus condenas; esa cooperación incluía atestiguar contra Knight Lighting. La Southem Bell estimaba el valor del E911 en setenta y nueve mil dólares, pero los abogados contratados por EFF demostraron que se vendía en las sucursales telefónicas a veinte dólares y, gracias a la colaboración de John Nagle -programador respetado y miembro de la WELL-, que había sido publicado con anterioridad en el libro The Intelligent Network (La red inteligente). También el periódico Telephone Engeneer and Management había dedicado un ejemplar al documento, con mas detalles que la publicación de Neidorf.

The Prophet tuvo que declarar por segunda vez y confesar que él había copiado el E911 de las computadoras de Bell South y se lo había enviado a Craig, quien no era miembro de la LoD y a quien nadie consideraba un hacker. El juicio a Neidorf se suspendió: no lo declararon inocente sino que se anuló todo lo actuado, se ordenó a los servicios secretos que borraran y destruyeran las huellas digitales, fotos, y cualquier otro registro del caso y Craig quedo en libertad, pero tuvo que correr con los gastos y costas, que sumaban cien mil dólares. El juicio fue público y los agentes federales no pudieron evitar que se divulgaran los métodos utilizados para controlar y obtener pruebas contra los hackers. La importancia fundamental que habían asignado a los BBSs radicaba en que -para ellos- están llenos de evidencias y controlarlos podía ser tan efectivo como pinchar una línea telefónica o interceptar la correspondencia. Sundevil fue el golpe mas grande de la historia a los BBSs. Los organizadores, el servicio secreto de Phoenix y la oficina general de abogados de Arizona consideraban que unos trescientos BBSs merecían la orden de búsqueda y captura, pero sólo consiguieron capturar cuarenta y dos entre el 7 y el 9 de mayo de 1990, además de veintitrés mil diskettes que contenían juegos pirateados, códigos robados, números de tarjetas de crédito, softwares y textos de BBSs piratas. Todos habían sido registrados de antemano, ya sea por informantes o por el servicio secreto.

La ola de indignación que se levanto por ese dato genero que Don Edwards -senador y miembro del subcomité de derechos civiles y constitucionales del congreso- junto a los Computer Professionals for Social Responsability (CPSR, Profesionales de la Computación por la Responsabilidad Social),

levantara un pedido de informes al FBI. La CSPR había nacido en 1981 en Palo Alto por la reunión de científicos y técnicos de computadoras a través de un correo electrónico, pero para 1990 contaba con mas de dos mil miembros diseminados en veintiún localidades de los Estados Unidos.

The Mentor (Lloyd Blankenship) estuvo bajo vigilancia un largo tiempo, pero su caso nunca llegó a los tribunales. La teoría del servicio secreto que lo involucraba en la edición de un manual se refutó al quedar demostrado que el escrito era un juego que comercializaría la Steve Jackson Games. El producto mas importante de esa empresa era el General Universal Role-Playing System (GURPS), que permitía que los jugadores crearan su propio juego de aventuras de rol. El proyecto sobre el cual trabajaba The Mentor era el GURPS Cyberpunk y el término era -para los agentes- sinónimo de hacking. Cyberpunk era el nombre adoptado por los escritores de ciencia ficción que en la década del 80 incorporaron a sus argumentos la evolución tecnológica informática y muchos hackers asumieron esa denominación como propia, identificados con los relatos de un mundo donde humanidad y tecnología ofrecían limites difusos. Si bien se secuestraron todos los equipos y periféricos que había en la sede de la empresa y en la casa de The Mentor, nunca se realizó una acusación formal ni se arrestó a nadie a pesar de que los servicios secretos demoraron mas de tres meses en devolver el equipamiento. Steve Jackson soportó pérdidas cercanas a los trescientos mil dólares.

The Urvile (Adam Grant) y The Leftist (Frank Dearden) fueron condenados a catorce meses de prisión, The Prophet (Robert Riggs) a veintiún meses y los tres debieron afrontar el pago de doscientos treinta mil dólares (por los dispositivos de acceso hallados en su poder, códigos de identificación y contraseñas de Bell South). Phiber Optic recibió como condena treinta y cinco horas de labor comunitaria y la LoD lo expulsó de sus filas por haber colaborado con demostraciones -junto a Acid Phreak- para un articulo de la revista *Esquire*. Phiber se unió entonces a los MoD, pero en diciembre de 1991 fue arrestado con otros miembros de la banda. Fry Guy tenia dieciséis años cuando lo detuvieron. Confesó que realizaba fraude con tarjetas de crédito pero mantuvo su declaración de inocencia en cuanto a las bombas y a las derivaciones de llamadas. Le confiscaron todo su equipo y quedó en libertad vigilada.

El Sundevil y Después

Uno de los personajes más activos durante el operativo Sundevil y que obtuvo gran espacio en la prensa de los Estados Unidos fue Gail Thackeray, asistente del fiscal de Arizona. Nadie en su momento pudo ignorarla, ya que fue quien pronunció las frases más propagandísticas sobre el operativo. "Los criminales electrónicos son parásitos -afirmaba-: de a uno no representan mucho daño, pero nunca aparecen de a uno. Vienen en grupo, legiones, a veces subculturas completas, y muerden. Toda vez que compramos una tarjeta de crédito hoy en día perdemos un poco de vitalidad financiera para dársela a una especia muy particular de chupasangre."

Gail no abandonó todavía su costumbre de perseguir a los hackers, aunque se queja por la velocidad con que se multiplican los elementos de telecomunicaciones y el grado de universalidad que adquieren mientras que los gobiernos y las policías no son globales. "Los hackers no merecen la reputación de Robin Hood -sostiene-; consiguen estadísticas de créditos y demográficas, pero despluman a los viejos y a los débiles."

Poco tiempo después del Sundevil, muchos de los involucrados se reunieron en la conferencia Computadoras, Libertad y Privacidad que se desarrollo en San Francisco entre el 25 y el 28 de marzo de 1991. Entre los cuatrocientos asistentes de la comunidad electrónica debatieron sobre el tema John Barlow, Gail Thackeray, Steve Jackson, Phiber Optic, Knight Lightning, Drake y Donn Parker, quien sostuvo que la categoría de crimen computacional desaparecerá porque "todos los delitos se harán por ese medio", según vaticinó.

Si buena parte de los norteamericanos creyó que la caída del sistema telefónico del 15 de enero había sido obra de los hackers, la realidad de esos servicios no tardó en demostrar lo erróneo de tal suposición. El sistema telefónico moderno depende de un software y todo hace suponer que la catástrofe de enero se produjo por una falla operativa. Según detalla Bruce Sterling en *The Hacker Crackdown* (“La campaña anti-hacker”), el nuevo programa instalado por la Telco tenia un terrible bug (error de configuración). Estaba escrito en lenguaje C con una función típica de programación, "do.... while..." ("hágase... mientras..."), donde se detallan los procesos que debe efectuar la computadora mientras se mantengan determinadas condiciones. Pero una de las lineas intermedias contenía la cláusula "if... break" ("si... detener"), aclaración que sirve para programar la interrupción de la rutina de procedimientos si sucede algo específico. Al parecer, en esa linea de código C estaba el error: cuando dos llamadas ingresaban en el mismo milisegundo a la central telefónica, esta cerraban el paso a las líneas, derivaban las llamadas a dos conmutadores diferentes, y hacían un respaldo de seguridad de sus datos de actuación en memoria para reparar los posibles errores. El problema sucedía cuando al terminar esta veloz rutina no encontraban un ruteo válido por saturación de las demás líneas telefónicas. En lugar de detenerse la acción, el sistema ingresaba en un bucle sinfín donde se dedicaban a hacer sus propios respaldos de memoria. El primer problema surgió en un conmutador de Nueva York y de allí se extendió a Atlanta, Saint Louis y Detroit, iniciando una acción de bola de nieve y arrastrando a todos los centros de conmutación telefónica durante horas.

En los siguientes dieciocho meses los sistemas de las telefónicas registraron dos caídas mas. Entre el 1 y 2 de julio de 1991, Washington DC, Pittsburg, Los Angeles y San Francisco quedaron sin servicio de teléfono y mas de doce millones de personas no pudieron comunicarse con otras ciudades. Los directivos de DSC Comunication Corporation de Plano, Texas, confesaron que la falla estuvo en el software de Bell Atlantic y Pacific Bell. El 17 de septiembre del mismo año hubo una falla eléctrica y las baterías preparadas para entrar en acción en esos casos no lo hicieron: tres aeropuertos quedaron incomunicados y se vieron afectados ochenta y cinco mil pasajeros. Los técnicos de AT&T no se encontraban en sus puestos en el momento de la catástrofe: estaban recibiendo clases sobre el sistema. Bruce Sterling sostiene en su texto que Sundevil, como cualquier operativo de gran envergadura, tuvo -mas allá de los escasos resultados en condenas firmes- intenciones políticas. Las quejas de los afectados por uso indebido de códigos telefónicos, tarjetas de crédito y telecomunicaciones, hasta ese momento, habían caído en saco roto por falta de oficiales capacitados en computadoras o porque los delitos de cuello blanco y sin víctimas carecían de prioridad en los asuntos policiales.

Sundevil fue un mensaje para ellos: alguien se preocupaba por la seguridad y de allí en mas actuaría cada vez que fuera necesario. Del mismo modo, y tal como lo señalo Gary M. Jenkins -director asistente del Servicio Secreto- , se les dijo a los hackers que "el anonimato de sus terminales" no servía

como escondite porque los agentes de seguridad patrullaban en el submundo de las telecomunicaciones, incluidos los BBSs.

También fue una señal para el FBI. Sus eternos rivales del Servicio Secreto podían llevar adelante una operación mientras ellos tomaban café en sus vasitos de plástico.

Los dos servicios de seguridad tienen jurisdicción sobre los delitos cometidos con computadoras si se producen en el ámbito federal, ya que el Congreso norteamericano decidió no otorgar primacía a ninguno. Por ultimo, la Unidad de Crimen Organizado y Extorsiones de Arizona, cabeza de la operación, demostró que era una de las mejores del mundo.

Los Hogares Hackers

Los BBSs, lugares de reunión de hackers que tanto preocuparon a los investigadores del Servicio Secreto, tenían para la época de Sundevil una larga tradición. En marzo de 1980 se conectó uno de los primeros que ganaron importancia por su contenido: el 8BBS, dirigido por Susan Thunder y El Cóndor, quien por sus actitudes concitó la indignación de las asociaciones underground. Fue detenido y encarcelado durante seis meses en un calabozo individual y aislado, dado el temor de las autoridades a que con sus intrusiones comenzara una tercera guerra mundial. Otro BBS, Plovernet, operaba en Nueva York y Florida y su *sysop* (operador de sistemas) era un adolescente: Quasi Moto. Atrajo a quinientos usuarios en 1983 y fue el primer hogar de la League of Doom; de hecho, durante unos meses su fundador Lex Luthor fue co-sysop, junto a Emmanuel Goldstein.

El Digital Logic Data Service de Florida era manejado por un tal Digital Logic, donde Lex Luthor concentraba gran reconocimiento. Los Neo Knight operaban el BBS Apple y Free Word II, el Major Havoc. Metal Shop, sede de PHRAC, fue uno de los pocos que funcionaron en Saint Louis.

La League of Doom comenzo a funcionar en 1984 nucleando básicamente a phreakers, entre ellos Lex Luthor, de dieciocho años por entonces, especialista en el Central System for Mainframe Operation (COSMOS), una red interna de Telco. Después se agregaron hackers y la lista de miembros se amplio a ControlC, Silver Spy, The Prophet, The Urvile, The Leftist.

Silver Spy tenia su propio BBS, el Catch 22, considerado como uno de los mas pesados de aquella época; ControlC fue buscado frenéticamente por la Michigan Bell, hasta que en 1987 lo detuvieron. Era un adolescente brillante y poco peligroso que no contaba ni remotamente con la posibilidad de pagar los importes acumulados en llamadas de larga distancia.

A pesar de todos los esfuerzos policiales por controlar y detener el hacking, el movimiento continúa su camino y va en aumento. Entre el 4 y el 6 de agosto de 1993 se efectuó el segundo congreso internacional organizado por los holandeses de Hack-Tic bajo el lema "Hacking at The End of The Universe" (Hackeando en el fin del universo). Rop Gonggrijp -quien también participo del congreso de 1989 en el centro cultural Paradiso, de Amsterdam- enfatiza las diferencias entre uno y otro. Los organizadores prefirieron para el segundo un lugar alejado de la civilización y así eligieron Flevoland, una de las doce provincias holandesas que todos llaman Flevopolder, porque es tierra ganada al mar. Carpas, sillas, mesas, barriles de cerveza e infinidad de cables ocupaban el terreno sede del encuentro, cuando encontraron una dificultad: necesitaban mas lineas telefónicas. La empresa local, PTT Telecom, les ofreció una solución: con un multiplexor podían darles ocho lineas en dos cables, aunque eso traía

una nueva complicación: no se podian pasar fax ni modem de alta velocidad. "Pero eso no es problema para una conferencia de este tipo, ¿verdad?, ironizaron los técnicos de PTT.

El congreso se inauguró con una charla de Emmanuel Goldstein y las sesiones se realizaron en talleres. Pengo explicó las debilidades del sistema operativo VMS; Billsf y Rop contaron que tipo de mensajes de radiollamado se pueden interceptar; David C. desarrolló los principios del dinero digital anónimo. Y todos se comunicaron con el resto del mundo vía Internet. La prensa -que en marzo, cuando los de Hack-Tic habían hecho el anuncio, no había dedicado ni una linea al congreso- se presentó en masa al advertir que la asistencia fija era de setecientas personas mas otros trescientos visitantes por día. Segun Rop, la segunda jornada en Flevoland tenía "un clima Woodstock; además, algunos tenían hashis o porro, que dejaban sus perfumes característicos en la carpa principal". Hubo quejas por la comida: era demasiado sana, protestaban los hackers, que preferían pizzas.

Un Mensaje

En noviembre de 1993, Phiber Optic se despertó en medio de una pesadilla: su casa estaba copada por agentes federales que revisaban cuanto cajón encontraban y separaban todo lo que tuviera que ver con computación.

Phiber no sabia que siete compañías telefónicas regionales de Bell, varias bases de datos de agencias del gobierno y otras empresas de comunicaciones como la Telecom Británica habían asentado una denuncia por intromisión no autorizada. "El juicio fue de los Estados Unidos contra mi persona", acusa Phiber Optic, quien recibió una condena de un año en prisión y salio en libertad el 22 de noviembre de 1994. Ese día sus compañeros de ECO, un sistema de conferencias, lo recibieron con una fiesta de bienvenida y lo reasignaron al trabajo que realizaba antes de ir a prisión: ocuparse de las computadoras, la base de datos y algunos aspectos técnicos, como las conexiones con Internet. A mediados de diciembre de ese año, Patrice Riemens, en camino de regreso a Holanda desde Buenos Aires, lo entrevistó en Estados Unidos.

- ¿Cual sería una buena ley sobre crimen computacional? ¿O no deberían existir leyes?- Interrogó Patrice.

- Obviamente hay crímenes con computadoras -reconoció Phiber- para los que debería haber leyes, pero en los Estados Unidos son muy confusas porque en 1986 las que existían fueron ampliadas para crímenes financieros, generalizándolas. Eso no sirve, son cuestiones muy distintas. En los casos de crímenes financieros, en los que hay grandes cifras de dinero involucradas, se llega a un acuerdo con las personas o con los representantes; en cambio, en computación eso no se da.

- ¿Por qué tantas empresas de teléfono se pusieron de acuerdo para acusarte?

- Las compañías quisieron enviar un mensaje: "No vamos a tolerar la entrada en las computadoras, no hay que meterse con ellas". En realidad, hacía ya diez años que las corporaciones sufrían infiltraciones, y lo mantenían en secreto.

- En causas anteriores los tribunales fijaron multas. ¿Cómo fue en tu caso?

- En mi caso una sola compañía, la Southern Bell, declaró un daño de trescientos setenta mil dólares; para llegar a esa cifra calcularon cuanto dinero se necesitaba para cubrir la seguridad de las

computadoras, algo ridículo. A mí no me multaron, pero muchos hackers tuvieron que hacerse cargo de cifras exageradas. Los tribunales también establecen períodos de libertad condicional en que tenés que trabajar para pagar las cuentas: yo, por ejemplo, tengo que hacer seiscientas horas de trabajo comunitario.

- ¿Cuál es el futuro del hacking?

- No sé hacia dónde van las cosas. Ahora hay gran interés por que se ignoren determinadas cuestiones, pero no siempre fue así. Hay quienes dicen que el futuro va a estar en manos de las agencias del gobierno y de las corporaciones y hay una visión mas optimista que dice que el individuo será cada vez mas poderoso. Sin embargo, las cosas están muy desorganizadas, hay cada vez menos personas que quieren hacer algo que las lleve a encontrar novedades, y esa es una de las razones del hacker.

- ¿Y cuál será el futuro de la Internet?

- Nos guste o no, crecerá y se comercializará cada vez mas. Hace poco hablé por teléfono con una gente que cree que el poder estará en manos de los individuos. Eso es por lo que peleo, algo que no existe ahora, y no me interesa mucho ir a la cárcel otra vez. Mientras estuve preso pensé mucho y creo que las personas se están convirtiendo en una especie de vagos que se sientan ante una computadora como a mirar televisión, sólo para ver imágenes, dibujos o leer noticias; se están convirtiendo en vegetales.

- ¿Seguirá de esa manera?

- Me temo que sí. Al ciudadano promedio no le interesa realmente la tecnología y muchos hombres de negocios se obsesionan en su tiempo libre con distintas herramientas, pero no se preocupan por saber cómo funcionan: simplemente, las desean.

La Difusión hacker

Como toda comunidad que reconoce intereses comunes y específicos, la de phreakers y hackers tuvo y tiene sus publicaciones. La primera -que divulgaba secretos para hacer phreaking- fue obra de una linea del Youth International Party (YIP, Partido Internacional de la Juventud) fundada por Abbie Hoffman: La YIPL (Youth International Party Line), cuyo primer número salio a las calles de Greenwich, Nueva York, en mayo de 1971. En colaboración con Al Bell, el mismo Hoffman diseñó una simple hoja en la que se enseñaba a manipular aparatos telefónicos como paso necesario para quebrar a las compañías telefónicas. El partido proponía el uso de los servicios públicos sin pagar y MaBell era, casi, el enemigo principal. Abbie tuvo que desaparecer varias veces por su actividad política y al fin dejó la revista en manos de Al, quien la convirtió en Technical Assistance Program (TAP), publicación con mas orientación técnica que política, que se dedicó a reproducir el material de Bell Telephone. A principios de los años 70, con el advenimiento del télex y las computadoras, Al delegó el manejo de TAP en Tom Edison, quien la dirigió hasta 1983, cuando un robo seguido de incendio intencional destruyó todas las instalaciones. Entre los medios electrónicos, la revista digital de mayor alcance fue PHRAC, que inició sus actividades el 17 de noviembre de 1985 en Metal Shop, un BBS operado por Taran King y Knight Lighting. En sus orígenes era una serie de archivos de texto que se distribuía sólo a través de Metal Shop, pero cuando los sysop obtuvieron acceso a Internet se desparramó por todo el

mundo gracias al servicio de e-mail (correo electrónico) que les permitió enviar cientos de copias automáticamente.

Invitaba a escribir archivos sobre phreaking, hacking, anarquía o cracking. El primer número incluyó un listado de dial-ups (número de acceso telefónico a computadoras a través de un módem) en el que estaban, por ejemplo, las universidades de Texas, Yale, Harvard, Princeton y el Massachusetts Institute of Technology (MIT). También explicaba cómo utilizar tarjetas de llamadas internacionales ajenas de la red norteamericana y listaba los códigos de treinta y tres países cubiertos por la compañía telefónica MCI. Sus colaboradores escribían también en 2600, y en el numero 24, de 1989, publicaron el documento E911, que originó el juicio a Knight Lighting. Hoy se considera que la aparición de PHRAC provocó una revolución en el underground informático: los hackers y phreakers más famosos -incluidos los miembros de la League of Doom- escribieron u opinaron en sus páginas.

Pocos meses después de la destrucción de TAP, Emmanuel Goldstein imprimió el primer número de 2600, The Hacker Quarterly, revista trimestral que retomó la tradición política de las publicaciones para el underground computacional. Desde 1987 y hasta la actualidad fue labrando la fama que la convirtió en una de las más importantes a nivel mundial: divulga métodos de hacking y phreaking, señala circuitos para trampear teléfonos e interceptar líneas, revela fallas de seguridad en los sistemas operativos, ofrece listados de dial-ups y mantiene una crítica permanente hacia quienes legislan y controlan el mundo de las comunicaciones. Salvaguarda su responsabilidad con la primera enmienda de la Constitución norteamericana, que garantiza la libertad de expresión; además, en todos los artículos técnicos se aclara que el fin de esa información es el estudio y el uso de los dispositivos es ilegal.

La revista adquirió tanta fama que vende por correo remeras, videos y otros objetos con propaganda; a veces organiza convenciones, aunque su director prefiere explicarlo todo de otro modo: "La gente se acerca y quiere reunirse. Eso es bueno. Nosotros les sugerimos un lugar público y céntrico para romper la idea que asocia a los hackers con criminales, y así se arman los encuentros".

La revista no es el único modo de difusión de el hacking elegido por Emmanuel Goldstein: tiene también un programa de radio los miércoles por la noche que se difunde en Manhattan y que concita aun mas atención que 2600. Goldstein visitó Buenos Aires para asistir al Primer Congreso sobre Virus, Computer Underground y Hacking que se realizó en el país.
"Se esta estableciendo un puente entre las nuevas tecnologías, la libertad de expresión y los derechos universales", sostuvo durante su corta estadía, para manifestar luego una esperanza: "Quisiera ver en el futuro a los individuos que ahora no tienen grandes conocimientos haciendo un uso mas intensivo de la tecnología. Para eso, los hackers debemos enseñar lo que sabemos".

- ¿No te escuchás un tanto soberbio?

- Puede ser. Si, algo de eso hay. Pero los hackers quieren comunicarse, quieren transmitir sus conocimientos. El problema es tener la capacidad y la habilidad para hacerlo. No es sencillo. 2600 existe, justamente para achicar esa brecha y poder explicar qué hacemos y cómo.

- ¿Era esa la intención inicial de la revista?

- No, para nada. Cuando empezó hacíamos veinticinco copias con la idea de comentar las novedades para los hackers. Despues creció y se convirtio en lo que es ahora.

- ¿Cómo no te controlan, no te persiguen, a pesar de lo que publicás?

- Creo que los organismos oficiales siempre están mirando lo que hacemos, pero yo hablo de como funcionan los sistemas: no incito a la gente a romper la ley. Tenemos muy claro cuál es el límite. No está prohibido explicar el funcionamiento de algo. Sucede que algunas personas no entienden de qué se trata y suponen que estamos haciendo cosas ilegales; es fácil decir que alguien conspira cuando no se sabe de que se esta hablando.

- ¿Las leyes reflejan esa confusión?

- Te cuento un caso específico: una persona entró en los sistemas, defraudó con tarjetas de crédito por medio millón de dólares, fue detenido pero nunca condenado; otro, que entraba en los sistemas de grandes corporaciones y miraba que pasaba, cómo eran, y está preso. Su alias es Phiber Optic y lo condenaron a un año de prisión por ser honesto y contar las cosas que veía. Cuando el juez leyó la condena aclaró que se lo había juzgado como a un símbolo, algo que no debería pasar en ningún país del mundo. Creo que hay que evitar las generalizaciones. Cuando un criminal usa una computadora dicen que es un hacker, y no siempre es así.

- ¿Qué hacen ustedes para evitar esa generalización?

- Es muy difícil evitarla, porque las computadoras pueden usarse para cometer crímenes. El error está en que la gente piensa que los hackers son los únicos que entienden las computadoras. La realidad es que casi todo el mundo tiene suficientes conocimientos de computación como para aprovecharlos en beneficio propio.

- ¿Ningún acto de hacking es ilegal?

- El hacking debe ser limpio; si uno hace algo ilegal, está bien que vaya a la cárcel. Lo de Phiber no es justo; su crimen fue decir públicamente lo vulnerables que son los sistemas.

- El movimiento hacker ya no genera grandes descubrimientos. ¿Se estancó?

- No, no creo. Hay maneras diferentes en que los hackers pueden desarrollar nuevas tecnologías; Steve Wozniak y Bill Gates fueron pioneros porque hasta ese momento no había computadoras personales, pero ahora hay otras cosas para hacer: nuevas máquinas, nuevo software.

- Aquellos primeros hackers eran, en su mayoría, técnicos electrónicos o estudiantes de ingeniería. ¿Cuál es tu carrera de origen?

- Ninguna. Cuando empecé a hackear estudiaba Bellas Artes. Nunca asistí a curso alguno de computación. No es necesario ser hacker para tener la mentalidad adecuada: todo se basa en curiosidad, en las preguntas. Hay muchos periodistas que podrían ser hackers si tuviesen una computadora a mano, porque la mentalidad es parecida: querer saber lo que antes no se sabía. Si hackeaste una vez, por otra parte, ya no podés dejar de hacerlo. Te podrán sacar la computadora pero jamás podrán impedir que preguntes.

IV. Sucesos Argentinos

"En los viejos tiempos las cosas eran mucho mas complicadas que hoy en día. En la época de la que estamos hablando había muy pocos módems y muy poca información. Era todo un trabajo a pulmón. Había que empezar de cero."

EL CHACAL, VIRUS REPORT I

- ¿Adónde quieren viajar?

- A cualquier lado, no te hagas el vivo.

- Okay. Digamos... Europa y... por Lufthansa, que es una buena empresa. Cuatro pasajes: dos para ustedes, dos para las patronas. Podemos endosarlos a Air France en... mmm... Chicago y de ahí derivarlos a... a ver, a ver... Lufthansa, en Nueva York. Esperamos un poquito y... ¡listo! Ya pueden ir a buscarlos a la sucursal de Lufthansa.

- Vos nos estas tomando el pelo, pibe, ¿no?

- ¡No! No, ¡de verdad! Mande a alguien, va a ver.

Los dos comisarios a cargo del interrogatorio se miraron. Habían escuchado una y otra vez, sin poder entender, las respuestas, cada vez mas elaboradas, a sus preguntas. No podían completar el cuadro: sospechaban, sentían que no se trataba de un acto legal; en ninguna figura penal, sin embargo, cabía ese episodio. Tal vez con un ejemplo, había propuesto el detenido. Aunque desconfiaban, decidieron tras la silenciosa consulta hacer la prueba. Uno de los comisarios ordenó:

- Che, Rodríguez, te me vas hasta Lufthansa y me averiguás si hay pasajes a nombre mío para Europa.

Minutos mas tarde el suboficial Rodríguez regresó, tickets en mano y aún incrédulo: "El mensaje tardó treinta segundos en entrar en la computadora de Lufthansa en Frankfurt". Era el 3 de marzo de 1983 y en alguna dependencia policial, detenido, Raúl Horacio "Yuyo" Barragán demostró -con el equipo de télex de la Policía Federal- cómo podía conseguir pasajes en avión sin demasiadas vueltas, y sobre todo sin pagar.

La historia de Yuyo comenzó en 1978, año del primer Campeonato Mundial de Fútbol del país, pantalla de la dictadura militar que lanzaba, como propaganda contra las denuncias del secuestro y la desaparición de personas, la consigna: "Los argentinos somos derechos y humanos". Yuyo tenia veintiún años y era un gerente contratado en la sucursal de Concordia, Entre Ríos, de la empresa

Aerolíneas Argentinas. Para su trabajo de ventas contaba con un teléfono y una terminal de télex conectada en forma directa por coaxil privado a Santa Fe, aunque durante la mitad del tiempo esa conexión no funcionaba.

El mecanismo de la venta de pasajes aéreos contemplaba -aun lo hace- que una empresa pueda entregarlos fuera del país de origen mediante otra compañía. Cuando se le presentaba uno de esos casos, Barragán informaba a la sede de Buenos Aires y esta se comunicaba con el Sistema Internacional de Comunicaciones Aeronauticas (SITA). De origen francés, esa organización se encarga de hacer las reservas de pasajes de todas las compañías aéreas del mundo: registra el pedido en su central de Inglaterra, lo confirma con la central de los Estados Unidos y luego da la orden de emisión en el lugar que corresponda. Por entonces las aerolíneas se pagaban entre sí los viajes que realizaban con otras cada seis meses.

- Tengo que confirmar estos pasajes como sea -urgió Yuyo a la operadora de télex-; la gente que me los pidió esta en Londres y es mucha plata ¿me entendés?

- Si, si -contesto ella-, pero todos los números de Aerolineas en Buenos Aires están ocupados. ¿Que querés que haga?

- Y... seguí probando mientras pienso.

Barragán decidió que intentaría saltear esa conexión en la Capital Federal. Buscó en las guías de trafico aéreo los códigos y claves que necesitaba y en la de télex el numero de SITA en Buenos Aires. Se comunicó, hizo la reserva con los datos de Aerolíneas y a los pocos minutos tenia la confirmación. En qué exacto momento Barragán supo que podía realizar las mismas o similares llamadas para hacerse de un pasaje sin pagar es algo que ya olvidó, pero recuerda que la primera vez involucró sólo a Aerolíneas Argentinas: generó un pedido con origen en Nueva York de un boleto por el sistema prepago. En la central de Buenos Aires nadie sospechó. La aprobación fue inmediata y sin dificultades. Falsear los mensajes de télex era, además, bastante sencillo.

Yuyo comenzó a noviar. Su amor era una empleada de la sucursal colombiana de Aerolíneas y, naturalmente, los pasajes gratis que le daba la compañía no alcanzaban para que pudiera visitarla todos los fines de semana, como ambos deseaban. Para probar la voluntad del enamorado, Yuyo envió una nota al presidente de Aerolíneas, con copia a su jefe directo, dando el permiso necesario para el feliz desarrollo del romance, aceptando pagar gastos y viáticos. El jefe se sorprendió, pero no tenía forma de saber que tanto el pedido de permiso como la aceptación eran falsos.

Con esos antecedentes y con su primer éxito, Yuyo perfeccionó su accionar y dejo volar -literalmente- su imaginación por el mundo. En 1982, en plena Guerra de Malvinas, pidió desde Rosario una ruta poco común a la empresa holandesa KLM, con origen en Tel Aviv. Como a raíz del conflicto esa compañía salía de Montevideo, el "cliente" de Barragán pidió endoso a Aerolíneas Argentinas para salir de Ezeiza.

- Pedí la confirmación a Buenos Aires -ordenó un jefe de KLM que olió algo raro.

- Allá dicen que nadie hizo el pedido -contestó el empleado un rato mas tarde.

- ¿Cómo? Confirmá con Tel Aviv, que es el lugar de origen.

- ¿De qué hablan? -preguntaron en Tel Aviv.

- Pero ¿qué pasa aca? LLamá a Rosario y averiguá de donde salió el pedido -ordenó el mismo jefe.

- En Rosario dicen que fue Tel Aviv -dijo el mismo empleado.

- Acá hay algo que no funciona...

Yuyo Barragán huyó hacia Brasil. A poco de llegar la falta de efectivo lo estimuló para volver a probar su sistema. Eligió a Varig para el primer intento y le dio excelentes resultados: se dedicó a revender pasajes a mitad de precio. A mediados de enero de 1983 el hermano de una prostituta amiga desconfió de la ganga y decidió hacer algunas averiguaciones en una agencia de empresa aérea.

- ¿Dónde lo compró? -fue la primera inquietud del empleado.

- Un tipo se lo vendió a mi hermana muy barato, a mitad de precio. ¿Sirve?

- Si, viene de la Eastern de Chicago y está confirmado por nuestra agencia en Copacabana. ¿Quién es el que se lo vendió?

La policía brasileña detuvo a Barragán esa misma noche. Los ejecutivos de Varig fueron a verlo y le propusieron entregar los códigos que utilizaba y explicar como era el sistema; a cambio, no harían ninguna denuncia. Yuyo aceptó con la condición de que el encuentro fuera a la mañana siguiente. Era tan tarde, estaba tan cansado. Pero ante todo la cortesía: esa noche, antes de salir en libertad, obsequió al comisario un par de pasajes y un cheque por su comprensión y sus buenos oficios.

Cuando a media mañana del día siguiente los empleados de Varig llegaron al hotel donde se hospedaba Yuyo no encontraron nada ni -lo mas importante- a nadie. El hombre había volado a Buenos Aires gracias a un pasaje San Pablo-Montevideo de la misma Varig que endosó a Iberia.

- El cheque lo denuncié como perdido antes de irme; además, no tenía fondos. No puedo volver a Brasil, claro: si me enganchan me meten adentro por cien años -supone ahora Barragán al recordar el episodio.

De vuelta en la Argentina siguió con el negocio, aceptando trueques además de efectivo. De esa forma obtuvo, en febrero de 1983, un lujoso Rolex. Pero el reloj no funcionaba. Lo llevó a arreglar y, en el momento de retirarlo, le exigieron boleta de compra que -por supuesto- no tenia. Otra vez lo detuvieron. Puesto a explicar como había llegado el reloj a sus manos, Yuyo decidió confesar. Demostró su manera de operar obteniendo los pasajes para los comisarios y sus señoras, pero tampoco así logro hacerse entender: la policía tuvo que consultar a especialistas internacionales que lo tradujeran. Los agentes del FBI enviaron un télex respondiendo -y a la vez preguntando- a sus pares de la policía argentina:

"Confirmado Lufthansa utiliza servicios SITA para circuito Bohemia-Long Island-Nueva York. Rogamos informe:
1) Cómo Barragán aprendió ese sistema;

2) más detalles sobre 'Delfo el mexicano';
3) cómo Barragán sabe que Cauma Travel Nueva York está involucrada;
4) qué otras agencias de viaje afectadas. Stop".

Seguramente la respuesta fue larga.

¿Porqué nunca se detectó la falsedad de las llamadas? Yuyo lo explicó ante la ley de esta manera: "Las líneas tienen muchas dificultades. No sé si habrán notado que casi siempre los pasajes vienen con un error en el nombre. Los que pedía para mi decían "BARAGAN", con una sola ere. Eso es basura del satélite y la gente de las compañías aéreas del mundo lo sabe. Ante cualquier inconveniente uno muestra el documento, se dan cuenta de que es un error de transmisión, y listo. ¿Qué hacia yo? Descubrí que si al final del mensaje metía una orden de retorno para el carro (equivalente al Enter de las computadoras) y en la línea siguiente ponía cuatro eles mayúsculas, cerraba el circuito. Doy un ejemplo: mandaba un mensaje a PanAm San Francisco ordenando un pasaje con origen en Milán para tal recorrido, a ser endosado a Aerolíneas Buenos Aires o a Varig Rio. El operador norteamericano que está mirando la pantalla lo ve entrar. Supongamos que se le ocurre verificarlo (cosa que casi nunca se hace): cuando va a intentarlo, se cuelga el sistema. ¿Cómo iba a saber que era yo el que lo hacía a propósito? Se quedaba convencido de que era un inconveniente de satélite y no desconfiaba. Tenía que apagar y reencender las máquinas, y para cuando terminaba de hacerlo ya se había olvidado".

A los cuatro días Yuyo salió del Departamento de Policía libre de culpa y cargo. Ninguna de las compañías involucradas en las sucesivas maniobras quiso presentar cargos ni se reconoció como damnificada: perder credibilidad ante los clientes era un daño superior al causado por Barragán. Las consultas generaron suficiente conmoción, sin embargo, como para que representantes de todas las empresas de aeronavegación realizaran un cónclave en París y tomaran algunos recaudos: cambiar todos los códigos, imponer mensajes de verificación y realizar el clearing cada treinta y dos días. Cuánto dinero gano Yuyo a lo largo de los años es algo imposible de determinar hoy, Ni siquiera él lo sabe con exactitud. Para las estimaciones oficiales fueron entre seiscientos y mil pasajes que, multiplicados por los cinco mil dólares que asigna SITA a cada uno, alcanzan cifras millonarias. Lo cierto es que no consiguió el famoso futuro asegurado. Ni siquiera un presente holgado.

Canto de Pericos

El cuarto mide seis metros cuadrados; tiene una ventana inalcanzable y un agujero en el lugar de la puerta. Las paredes están descascaradas y huele a humedad. Hay cinco mesas con algunos bancos largos, dos de ellos ocupados. La gente habla en voz baja. Yuyo llega con otro banco y una bolsa de compras de la que va a sacando yerba, azúcar, un termo y un cuaderno. Está ansioso: saluda efusivamente, no puede dejar de hablar mientras prepara el mate.

- ¿Cuanto tiempo hace que estás preso?

- Desde abril del '94. Pero pienso que voy a salir pronto. ¿Saben porqué me engancharon? Porque quería votar y fui a regularizar el domicilio.

- ¿Cuánto te dieron?

- Tres años. Lo más lindo es que fue por la causa del '82, que ya está perimida.

- Entonces, ¿cómo te detuvieron?

- No, no. Me detuvieron por otra cosa. Yo tengo dos causas, pero en la última todavía no hay sentencia.

- ¿Cuál es?

- La de Los Pericos.

- ¿Los Pericos, la banda?

- Ajá. Ellos hicieron en el '93 una gira por América: viajaron de acá a Caracas, a Miami, a Chile y el regreso. En Caracas descubrieron que los pasajes que usaban eran robados y se inició una causa. El representante de ellos dice que yo le vendí los pasajes, y acá estoy. Tienen que hablar con mi abogado para que les dé los expedientes, está todo ahí. Pueden verlos en el fin de semana y el lunes vienen a verme, así les aclaro lo que no entiendan.

Yuyo se siente solo y exige la promesa de una próxima visita. Su familia está en Entre Rios y, paradójicamente, no le resulta fácil viajar. De todos modos, él prefiere no verlos mientras esté en la Unidad 16 de Caseros. Renueva el mate y sigue hablando casi sin pausas, a pesar de que lleva ingeridos -asegura- dos Lexotanil y un Valium.

El abogado es un hombre muy ocupado y tan poco claro como su cliente. Después de mucha insistencia entrega fotocopias de un puñado de páginas, sólo de uno de los expedientes. Suficientes para saber algunas cosas.

Pablo Andres Urbano Hortal, representante de Los Pericos, aduce que compró los pasajes a Barragán de buena fe y que por eso no tiene recibo del importe abonado, unos veintidós mil dólares. Junto con los boletos se llevó la promesa de que al día siguiente le sería entregado el recibo correspondiente. En una rueda, Urbano Hortal reconoció a Yuyo como el hombre que le vendió los pasajes. Pero otro miembro del grupo que estuvo en el momento de concretar la operación no pudo reconocerlo.

El juez Juan Jose Galeano -el mismo que investiga el atentado a la AMIA y que generó un sumario para averiguar quien le había robado un sándwich de pan pebete, jamón y queso- parece creer en la palabra de Hortal. Decretó la prisión preventiva y reconoció el modus operandi de Yuyo. Sin embargo, hay una diferencia fundamental: los pasajes fueron robados de las agencias norteamericanas, mientras que Barragán se dedicó a lograr la emisión legal -con pedidos falsos- de acuerdo a la rutina de las compañías de aeronavegación. Yuyo esta en Caseros porque hay otras causas en su contra que lo convierten en reincidente y obligan a que cumpla la reclusión preventiva. Una de ellas corresponde al cierre de Bahía Compañía Internacional de Viajes, agencia que Barragán reabrió en Concepción del Uruguay cuando Aerolíneas Argentinas le canceló el contrato. A falta de dinero, saldó sus deudas con pasajes del sistema prepago. En el proceso por la liquidación del negocio lo condenaron a un año y seis meses de prisión, que no cumplió por ser la primera. El auto de resolución de Galeano cita otro antecedente judicial en el que la fiscalía pidió tres años de prisión. Según Yuyo, el proceso es de 1982 y las figuras son tentativa de defraudación a la administración pública -por haber engañado a Aerolíneas Argentinas para que emita pasajes a favor de ocho particulares con diversos destinos- y estafa en perjuicio de los compradores de esos pasajes. El 28 de diciembre de 1994 el juez Martín Irurzún dictó sentencia en el caso, estableció una condena de seis meses, la consideró cumplida por el tiempo que

Barragán había pasado detenido y ordenó su inmediata libertad en la causa. Pero aún debe esperar el fallo en el expediente de Los Pericos. Yuyo dice que su encarcelamiento "es una venganza de la policía", confunde hasta lo imposible las causas en las que está procesado y acusa al juez de haberlo condenado sin investigar: "Yo digo en el expediente que tengo una cuenta en Londres con un millón de libras y ni siquiera lo verificaron", afirma, como único argumento.

- ¿Es cierto? ¿Un millon de libras?

- Y algo más. Lo que pasa es que antes de que me detuvieran bloqueé todo. Por eso ahora no puedo usar la cuenta y estoy sin un mango. Acá tenés que pagar por todo: te dan algo para que te hagas la comida y el resto... a comprar.

Barragán comparte la celda con otros once detenidos. Tienen una cocina para preparar los alimentos (que reciben crudos) y un único baño para los doce. A modo de lujo poseen un equipo de música y algunos televisores, todos blanco y negro, excepto el de Yuyo. Eso le causa problemas, lamenta, porque su pasión por los informativos no es compartida por sus compañeros.
"El otro día al mediodía uno me pidió que lo dejara ver los dibujitos y le contesté que estaba mirando el noticiero. ¡Para qué! 'Má si -me dijo-, metete el televisor en el culo! Te pasás todo el día con lo mismo...' Claro, es difícil convivir acá. Cualquier cosa te pone nervioso ¿no? Al final le pedí disculpas."

- ¿Están todo el día en la celda?

- Sí. Tenemos una hora por día de recreo en el patio, y el resto del tiempo, adentro. Yo zafo porque me enganché con la Universidad: estoy haciendo el Ciclo Básico para seguir Abogacía. Ayer tenía que rendir un exámen y no me presenté, no porque no supiera, sino porque así sigo yendo todas las mañanas.

- ¿Qué hacés ahí?

- Qué se yo, leo, estudio. Por lo pronto puedo sentarme ante una computadora, y voy aprendiendo.

No bromea. Yuyo no es un genio de la computación: cuando comenzó con sus travesuras, él sólo entendía de picar cintas de télex. Pero se hizo una reputación. "Es un hacker desde todo punto de vista", define El Chacal, un colega también veterano del hacking patrio. "Lo que hizo es reloco. Desde Argentina, cuando ni se hablaba del magiclick! Es un pionero. Y es mas valioso porque no hay registro de que otra persona haya hecho por entonces algo parecido en ningún lugar del mundo; a lo mejor ser único lo puso en esta situación, tan difícil. Pero sobre todo lo que hay que rescatar es el hacking: él pudo hackear un sistema sin nada. El peligro -reflexiona El Chacal- es que lograrlo te hace sentir poderoso, y el poder es adictivo."

Una Red Gauchita

Recién en 1981 la Argentina se convirtió en un país con el cual, de haber interés en otro, intercambiar transmisiones de datos: la empresa norteamericana que operaba las redes Telenet y Tymenet instaló un nodo (una máquina que actúa como una sucursal bancaria) en Buenos Aires, informalmente bautizado CIBA por encontrarse en la Central Internacional Buenos Aires. Con ese estímulo, y a finales del año

siguiente, la entonces y única compañía telefónica estatal argentina, ENTel, inauguró la primera red de datos nacional, ARPAC, que unió localidades de todo el país y abarató las comunicaciones entre sucursales bancarias, casas de turismo, empresas y particulares necesitados de hacer circular información dentro del país. Se usó tecnología de punta, tan de punta que era desconocida en el mundo: los ganadores de la licitación para instalar la red, creadores de la española IBERPAC, tenían un nuevo diseño pero nunca lo habían aplicado. De experiencia, ni hablar.

La flamante red argentina, como todas las del mundo, tenia dos usos: local e internacional. Las transmisiones locales se hacían desde un nodo o a través de un módem de ARPAC y se facturaban donde las recibían. Las internacionales requerían que el usuario tuviera un nodo propio (una linea conectada directamente con ARPAC) o, si utilizaba módem, una clave IUR (Identificacion de Usuario de Red), NUI (Network user Identification) en inglés. Las claves tenían un modelo. N913066789/AB123, por ejemplo, debe interpretarse de un modo no demasiado complicado: N9 es el código del país: 1, el de telediscado de Buenos Aires; 3066789, el teléfono al cual se facturaba la utilización de la cuenta; AB123, la contraseña secreta del usuario (password).

ARPAC era -y es- una red de norma X.25, capaz de comunicarse con otras de ese tipo en todo el mundo. Algunas de ellas brindaban el servicio de outdials: computadoras con un módem instalado que permitían salir de la X.25 y entrar en la red telefónica para comunicarse dentro de un área local. Si el servicio era global outdial (GOD) permitía algo mas: llamar a cualquier teléfono del mundo.

Por entonces, sólo unos pocos privilegiados podían gozar del discado directo internacional (DDI), y en cualquier caso las llamadas de larga distancia cargaban tarifas exorbitantes. El uso -abuso, quizas- de ARPAC era una vía para acceder a bases de datos foráneas, como Dialog: la tentación de llamar al exterior y conseguir las últimas novedades en software o comunicarse con gente de otros países era, para algunos, difícil de resistir. Era, en fin, superior a la noción de culpa que puede acompañar a la ejecución de actos dudosamente legales. "Las redes de datos ofrecen varias aplicaciones: el correo electrónico, por ejemplo, llamado e-mail, que deja mensajes en una computadora en tiempo y periodos (el destinatario los recibe algunas horas después de emitidos) y no es interactivo; la posibilidad de conectarse a otras redes, como General Electric; el acceso a un banco de datos, un lugar donde se acumula información. El más famoso era Dialog -del cual yo era el representante-, una biblioteca informatizada con todo lo disponible en el mundo: cualquier libro o revista se incorporaba a ese banco de datos." Armando Parolari, ingeniero electricista, no sólo era la cara visible de Dialog en el país sino también para los usuarios de servicios internacionales, la de ARPAC. Dada su doble faz, prácticamente todos los que conocían la red nacional a través de él pensaban que sólo se podía acceder a Dialog.

A fines de 1985, impulsado por la necesidad de actualizarse en su disciplina, el padre de Alejandra resolvió contratar el servicio de ARPAC para comunicarse con los Estados Unidos, acceder a Dialog y realizar búsquedas bibliográficas en la National Library of Medicine. El médico encargó a su hijo de catorce años (varón, contra lo que podría suponerse de su alias femenino), el único de la familia que se llevaba bien con la computadora, la tarea de solicitar las cuentas en ARPAC, CIBA y Dialog. Dos meses más tarde Alejandra conoció a Parolari.

- Tenés que tener dieciocho años para abrir una cuenta - le advirtió el ingeniero.

- Bueno... puedo traer a mi hermano para que firme.

- Okay. ¿Y qué querés? ¿ARPAC?, Telenet o Tymenet?

- ¿Cuánto cuestan la conexión y el mantenimiento de cada una?

- Nada. Sólo se paga lo que se usa.

- Entonces quiero las tres.

El entusiasmo y la inocencia de Alejandra -y la generosa confianza de su padre- hicieron que en un mes después dispusiera de las tres cuentas. Al principio no se diferenciaban, ya que si bien el acceso a ARPAC era a 1200 Baudios y el e las otras a 300, la Epson QX10 del chico apenas tenía un módem de 300. Entonces los de 1200 eran escasos; los de mas velocidad, sólo un sueño para la mayoría de los usuarios locales. El nombre de usuario en Telenet era ENARGXXXNET y en Tymenet LRARGXXXRS; las XXX representan tres números, distintos para cada cliente. En ENTeL le asignaron a Alejandra una única password para las dos cuentas que allí tenia: su apellido. Nada original, por cierto. Ni seguro: cualquier persona que supiera cómo funcionaba la asignación de claves sólo debía probar las combinaciones posibles de números (mil, en esa estructura) y poner el apellido como password. Con un programa automático, como el Discador tipo Juegos de Guerra, se podía conseguir en una noche. La clave de ARPAC era mucho mas segura: la elegía el usuario y, si resultaba mala, era su responsabilidad. Alejandra intentó usar las cuentas para acceder a Dialog, pero se topó con las instrucciones de uso de ARPAC. En la fotocopia de una carilla mecanografiada -y no demasiado prolijamente- se leía:

```
"INSTRUCCIONES PARA ACCESO TELEFÓNICO A
 SERVICIO INTERNACIONAL DE DATOS ARPAC:
 En Buenos Aires únicamente:
 Discar 394-5430
 Recibirá tono de datos.
 Accionar dos puntos y Return o Enter.
 (Existiendo temporización, luego de un corto período se
 libra y se debe volver a discar.)
 En la pantalla aparece ARPAC".
```

La hoja seguía explicando como usar el IUR (Identificacion del Usuario en Red). La afirmación "Recibirá tono de datos" resultó ser una expresión de deseos, ya que en sus orígenes ARPAC tenía una sóla línea disponible y lo mas probable era recibir tono de ocupado. Una vez conectado, conseguir el famoso mensaje ARPAC era una misión imposible para Alejandra quien, armado de paciencia y ganas infinitas, volvió a hablar con Parolari.

- Debés estar haciendo algo mal -sentenció el ingeniero.

- Pero no, si sigo las instrucciones al pie de la letra: pongo el dos puntos y el Enter y no pasa nada.

- ¡No te digo! ¿Viste que estabas haciendo algo mal? No es la tecla de los dos puntos sino dos veces la tecla del punto.

Impaciente por debutar, por fin, con su cuenta de Dialog, Alejandra volvió a la oficina de su padre pensando en la calidad de los manuales de ENTel. La traducción de Parolari funcionó y Alejandra logró que ARPAC apareciera en su pantalla. Pero el entusiasmo por el chiche nuevo duró poco: si bien ARPAC tenía un precio razonable, cada consulta bibliográfica era carísima. Por eso Alejandra decidió usar el módem para acceder a los pocos BBSs locales, donde conoció gente que le abrió las puertas a otro mundo.

- Conseguí un programa buenísimo -le ofreció un día un amigo-. Te lo paso cuando digas.

- ¿De donde lo sacaste?

- De un BBS de Estados Unidos.

- Ahh. Sí, hay cosas bárbaras, pero el DDI es tan caro...

- Yo me comuniqué por ARPAC. Si querés, te puedo explicar cómo se hace.

Así obtuvo Alejandra el primer outdial que le permitió acceder a los BBSs de Miami. Como su interés principal era seguir ayudando a la oficina de su padre, pensó usarlo para comunicarse con científicos en Estados Unidos. Pero estaba limitado a Miami. Para conseguir mas outdials visitó a su proveedor oficial.

- ¿Qué? ¡No puede ser! ¿Quién va a ser tan idiota para dar gratis semejante servicio? -recuerda el joven la respuesta.

Parolari no sabía que servicios como PC Pursuit hacían justamente eso y que se trataba de una excelente forma de aumentar el tráfico de una red de datos. Las máquinas de PC Pursuit permitían la comunicación por módem para usuarios con tarifas preferenciales, mas económicas que las de larga distancia. Por ejemplo, un usuario de California pagaba en ese momento veinte centavos por minuto para una comunicación que cruzaba los Estados Unidos. Por medio de este sistema pagaba casi la mitad.

El descubrimiento de los outdials brindaba grandes satisfacciones a Alejandra pero la cuenta de ARPAC subía y subía. Cuando un hacker amigo le contó que se conectaba durante horas para traer programas sin aumentar su cuenta con la red, el asombro se dibujó en la cara del muchacho.

- ¿Cómo? ¿Hay otra posibilidad? -preguntó.

- Claro. Anotá: N91...

- ¿De dónde sacaste eso? Es una clave. ¿De quién es?

- No sé ni me interesa. Simplemente usala.

Alejandra entró en el underground. Primero usó la clave con temor, consciente de la existencia de un dueño y porque sabía el costo. Pero un día le dijeron que pertenecía a una empresa grande: "Con lo que deben gastar... si se la uso un poco no se van a dar cuenta", se justificó. No sólo se comunicaba con científicos en los Estados Unidos, sino que consiguió programas de dominio público y -entre otras cosas- el número de una máquina en Metz, Francia, cerca de la frontera con Alemania. Ahí se reunían

hackers de todo el mundo para charlar. Era QSD, un sistema en línea que permitía charlas en tiempo real con una gran capacidad de usuarios al mismo tiempo. QSD estaba conectado a Minitel -red telefónica francesa-, montado en una computadora ITMT con sistema operativo UNIX, y se podía acceder a través de Infotel -redes de datos en los Estados Unidos- o directamente por vía telefónica. Al ingresar, cada uno debía elegir un nombre para identificarse ante los demás participantes. Alejandra decidió pasar por mujer porque los hombres eran mayoría, todos querían comunicarse con "ella". QSD fue su adicción; llegó a estar conectado seis horas seguidas. Una de las personas con las que charló poco después de la Guerra del Golfo era un israelí, quien le contó cómo habían caído las bombas a seis cuadras de su casa, en Tel Aviv. Le mandó una carta a Alejandra y el chico decidió confesarle la verdad sobre su sexo, para evitar males mayores. Nunca más supo del israelí.

Las claves de ARPAC duraban meses; cuando dejaban de funcionar, siempre alguien tenía una que le habían pasado. Alejandra las usó sin preocuparse demasiado. Pero la diversión llegó a su fin. Cuando faltó una password ajena dando vueltas, Alejandra pensó en usar la suya y, para ahorrar el costo de las llamadas, traer mensajes de los Estados Unidos a Fido (una red mundial de BBSs que tiene un inconveniente: a veces, los envíos tardan semanas en llegar a destino). Escribir un programa para conectar el correo de Fido a través de ARPAC requiere conocimientos técnicos que Alejandra no tenía. Pidió ayuda a un amigo programador y operador de un BBS. Mientras hacían las pruebas, ese programa -que contenía la clave de Alejandra- iba y venía por módem de la casa de uno al BBS de otro. En uno de esos viajes el archivo quedó por error en un área de acceso público del BBS, un hacker lo vió y lo bajó. Fue el comienzo de una catástrofe. Alejandra pagaba por su cuenta de ARPAC unos cien o doscientos dólares por bimestre. De inmediato la cuenta subió a quinientos. La factura siguiente a mil y la otra a tres mil. Conocedor de lo que había pasado y con la segunda boleta abultada en la mano, fue a hablar con Parolari para cambiar su clave.

- Imposible -decretó el ingeniero.

- Entonces déla de baja -rogó Alejandra.

- Como quieras, pero eso tarda mucho.

- Escúcheme, me están usando la cuenta. Algo tengo que hacer.

- Bueno, hablá con mantenimiento técnico.

No tuvo mejor suerte. "La clave ya esta registrada en la computadora y no tenemos posibilidades de cambiarla ni de darle de baja", le dijeron. Después de dos semanas y de mucho discutir le informaron que todas las altas y bajas se hacían una vez por mes y acababan de hacer una, debería volver al mes siguiente. Esa vez fue la vencida: al mes siguiente consiguió que le cancelaran la cuenta en el momento. Alejandra cree que ese trámite engorroso para dar de baja una cuenta ayudaba a que las claves fluyeran por el medio. Todos podían, en mayor o menor medida, tener acceso a, por lo menos, una. "Después de eso -recuerda-, utilicé passwords ajenas lo mínimo indispensable, sólo cuando necesitaba comunicarme con alguien. Mi cuenta de Dialog ya había sido dada de baja". Tampoco podía negarse a pagar, tal como amenazó, porque la respuesta fue siempre contundente: "Si no pagás te

cortamos la línea". El lema de ENTel era "Pague ahora, reclame después" y en aquella época una línea podía esperarse diez años o mas. Alejandra tuvo que pagar hasta la última cuenta de teléfono.

Pinchaduras

A principios de 1983 -cuando Barragán estaba a punto de ser detenido y llevaba tiempo incursionando en las redes de télex de las compañías aéreas- El Chacal despertó una mañana con las voces de la televisión.

El programa que se emitía era Telescuela Técnica, y en ese episodio hablaban de los primeros ordenadores que llegaban al país. Mientras desayunaba se le impuso la obsesión por tener una computadora y no cejó en su empeño hasta conseguir, poco después, una TI99. "Así fue como empecé a incursionar por ahí", cuenta.

- Pero no todo el que se compra una computadora deriva en hacker...

- Claro, depende de cómo te acerques a ella. Yo la veía como una posibilidad de crear, me permitía acceder a un universo de 4K... Dios! Era algo maravilloso. En aquellos años no debíamos ser mas de veinte los que teníamos una computadora.

El Chacal se refiere, claro, a la memoria de la computadora, la capacidad de almacenar información, que se mide en kilobytes (K). Un kilobyte equivale a mil veinticuatro caracteres. Entre los modelos de aquellos años, los de 4K eran casi un privilegio, ahora las más comunes cuentan con 16.000 K. El Chacal empezó a hackear intuitivamente: nadie le explicó nada, no había de dónde sacar información. Pero en poco tiempo descubrió que mediante un simple llamado telefónico y algunas claves adivinadas podía salir de los limites físicos del país y acceder a computadoras lejanas, aunque afirma que, ya en aquel entonces, "no se podía hacer demasiado por la infraestructura telefónica".

Un cable que pasa cerca de la ventana de un departamento es una invitación a un mundo nuevo y fascinante. A fines de 1986 El Chacal y sus amigos Doctor Trucho, Goblin y Adam tomaron la costumbre de reunirse en la casa de Adam (la de la tentadora ventana), robar una línea telefónica para llamar a BBSs de todo el mundo y conseguir programas desconocidos en la Argentina. La ingeniería social los proveía de los datos necesarios.

- El único que tenia buena voz para eso era el abuelo -dice Adam, quien en aquel tiempo declaraba quince años.

El Chacal, confiado en su facilidad de palabra y su voz segura, elementos indispensables para sonsacar información valiosa a un desconocido, hacía sonar el teléfono de la víctima.

- Buenas tardes, señora. Le hablo de la central República de ENTel. Por favor deme su número de abonado.

- ¿Número de qué?

- Señora, por favor, ¡no nos haga perder el tiempo! Necesito su número de teléfono -impresionaba, con fingida impaciencia-: se cortó un cable y estamos tratando de restablecer el servicio.

- Ah, bueno, el numero es 40-3456.

- Muchas gracias. Va a notar que su teléfono no funcionará por unas horas, pero el inconveniente será solucionado a la brevedad. Mandamos una cuadrilla. Estamos trabajando para usted.

Cortaba y, al mismo tiempo, desconectaba al abonado. "Teníamos el número: gran algarabía y jolgorio. Seguro que nos prendíamos un porro", recuerda Adam. A continuación llamaban a la operadora:

- Hablo del 40-3456. Necesito hacer una serie de llamadas internacionales. La va a atender un fax, así que páseme directamente.

Así accedían sin costo (para ellos) a distintos BBSs del mundo. Si el teléfono tenia DDI (algo raro en esa época), todo era mucho mas sencillo. Pero no tuvieron en cuenta las horas de abuso de una línea: el usuario que pagaba por esas comunicaciones hizo la denuncia ante ENTel y el asunto llegó a manos de la policía. Cuando los agentes del orden vieron que los destinos de las llamadas estaban diseminados por todo el mundo, llegaron a una conclusión que les pareció obvia: narcotráfico. El caso era tan sospechoso que la feria judicial de enero no los detuvo. Llamaron a los 276 números listados en la cuenta telefónica y en todos lados les contestó un silbido agudo, señal de conexión de un módem. Excepto en uno.

- Lo llamamos de la Policía Federal Argentina. Estamos investigando un posible ilícito, y necesitamos su cooperación. ¿Cual es su nombre?

- Pedro Gonzales.

- ¿Recibió alguna llamada de la Argentina últimamente?

- Si.. de mi amigo Juan, hace unos días.

Todo el peso de la ley cayó sobre Juan, cuyo único pecado fue tener un hijo con amigos hackers. Estos le habían hecho el favor de comunicarlo con el hijo de Pedro, sin saber que la llamada de los padres, totalmente legal, los iba a delatar. El error fue llamar a un amigo: de haberse limitado a los módems, no hubieran podido rastrearlos. A pesar de que Juan vivía a dos kilómetros de la casa de Adam, donde se hacia la pinchadura, tuvo que pagar la cuenta que ascendía a unos quince mil pesos.

Piratas Patrios

Tal como sucedió en otras partes del mundo, las actividades de EL Chacal y Doctor Trucho tuvieron mayor resonancia cuando, junto a un par de colegas, formaron una banda: la PUA, sigla que no significaba otra cosa que Piratas Unidos Argentinos. A pesar de las reminiscencias de lunfardo de ese nombre y algunos alias -que obedecían a una etapa nacionalista de Trucho- ellos gustaban definirse como "ciudadanos de las redes". Según un relevamiento de la Subsecretaría de Informática y Desarrollo, en 1986 había en el país 63 bases de datos, 37 desarrollándose y 14 proyectadas. En el momento pico de actividad de la banda, 1987, las redes y bases de datos nacionales, pero sobre todo CIBA, Delphi y ARPAC, supieron de sus andanzas. Cuando El Chacal y Doctor Trucho descubrieron un número de teléfono en Buenos Aires donde los atendía un módem, comenzaron su relación con el hacking. Se trataba de una entrada a la red interna del Citibank que comunicaba entre sí las sucursales y

no permitía acceder a otros lugares. Por lo menos en teoría.

- Entrar en el banco era difícil, había mucha seguridad. De todas formas, no creo que, de haber entrado, hubiésemos sabido qué hacer. Pero en una sucursal, no me acuerdo cual, había un error de configuración. De ahí se podía salir a la red X.25 mundial, y pudimos conectarnos con algunos lugares -recuerda EL Chacal.

Poco después los PUAs fueron en patota a la Infotelecom de 1987 en el Sheraton Hotel para ver las demostraciones de uso de las redes como Delphi o ARPAC. La mayor parte del tiempo se aburrieron, pero encontraron a un operador que enseñaba cómo ingresar en algunas bases de datos y, mientras escuchaban, trataron de memorizar cada paso. En un momento el operador se distrajo y en la pantalla apareció una secuencia de números y letras.

- Dale, anotá, anotá -dijo Doctor Trucho al oído de El Chacal

- Vamos a probarlo.

- Pará, pará. No salgamos corriendo. Sería sospechoso.

La paciencia tuvo un fruto accesorio: al poco tiempo apareció otra clave. Ya convencidos de que no se llevarían nada más, fueron a probar lo que acababan de encontrar. Eran las contraseñas de la empresa FATE para usar ARPAC y CIBA. Esos fueron los comienzos. A mediados de 1987 Siscotel S.A., empresa comercializadora de Delphi -un sistema en linea local que proveía acceso a bases de datos de los Estados Unidos-, realizó una denuncia judicial: alguien estaba usando su cuenta de ARPAC. Había recibido una factura telefónica de cuarenta mil pesos, con un detalle de llamados que negaban haber realizado. En octubre, los PUAs se atribuyeron el hackeo en una nota periodística, lo que desató una investigación policial y revuelo en la prensa nacional.

- En el tiempo de vida de Delphi hemos detectado cuatro casos de piratas en el sistema -decía Alberto Antonucci, directivo de Siscotel-, pero no entremos en la ciencia ficción y en otro tipo de supersticiones, por favor. Este tipo de hacker que pintan algunas publicaciones, no sólo en nuestro país, no existe. Científicamente no puede existir. Nuestro sistema tiene dos entradas: el nombre que usa el usuario, que puede ser el real o un alias, y la clave. La primera no es muy difícil de averiguar porque existe un listado, la segunda es una secuencia de letras o números que puede ir de seis a treinta caracteres.

- Bueno, pero se sabe que prueban combinaciones.

- Si Delphi no reconoce la clave por tres veces consecutivas, corta la comunicación. A la quinta intentona (decimoquinta clave) que no es correcta, ademas de cortar, cancela la cuenta y se cita al titular para que de una explicación, o para advertirle que sucede. En los cuatro casos que tuvimos hubo errores por la falta de costumbre en el uso. Cuando decimos que la clave es secreta, debe ser eso, debe conocerla sólo el titular.

- En este caso usaron la clave de su empresa, ¿Cómo lo explica?

- Suponemos que la filtración se produjo en una exposición anual que realizamos en un hotel de Retiro. Pedimos una línea telefónica especial para el stand donde se hacían las demostraciones con el servicio Delphi de los Estados Unidos. Deben haber mirado y estudiado el movimiento de los dedos del operador sobre el teclado para averiguar la contraseña.

En el mes de mayo de 1987 ENTel había otorgado a Delphi la NUI (Network User Identification) especial que dejó de usarse en junio, cuando terminó la exposición. En diciembre y los meses siguientes, llegaron a la empresa facturas que detallaban: 1 de enero, uso de linea con Canada desde 11:30 a 15; desde 12 a 14 con Suiza. Otro directivo de Siscotel, Manuel Moguilevsky, había recibido en su cuenta personal de Delphi una carta electrónica firmada por PUA proveniente de la cuenta de la red Globo de Brasil. Los hackers aseguraban que no estaban vinculados con el caso, advertían acerca de otros grupos que se dedicaban a romper los sistemas y deploraban el dinero que Siscotel adeudaba a ENTel. "PUA usa sólo cuentas de empresas en forma distribuída para no recargarlas y quedar al descubierto", afirmaban. La policía se centró en la búsqueda de PUA e investigó los listados de llamadas hechas con el NUI de Delphi. Con la colaboración de Interpol trataron de localizar a los destinatarios, pero ninguno de ellos colaboró con la investigación por problemas legales que les impedían dar información sobre sus abonados o porque no había manera de identificarlos. Las comunicaciones se habían realizado con la Escuela Politécnica Federal de Zúrich, Suiza; una central para llamadas locales en la provincia de Alberta, Canadá; el Instituto de Matemática de Alemania; el Servicio de información de Datos de Hong Kong; General Electric y Compuserve en Estados Unidos. Los investigadores no pudieron avanzar más allá y todo quedó en la nada. Algunos expertos dicen que, de haber identificado a los verdaderos responsables, no hubiera sido posible enjuiciarlos debido a la falta de legislación adecuada en la Argentina.

Mientras se realizaba la pesquisa por el hackeo, los miembros de la PUA dejaban mensajes al sysop de turno en Delphi para que les abriera una cuenta a nombre de la banda y se comunicaban con la cuenta del periodista Enrique Monzón, quien al fin les hizo un reportaje que ocasionó la investigación para tratar de identificarlos. El Chacal recuerda que el sistema de Delphi tenía una falla: bajo ciertas condiciones particulares, en el momento de la conexión y antes de pedir la identificación, mostraba los usuarios que estaban en linea, con lo que brindaba la oportunidad de averiguar nuevas passwords para futuras llamadas. "Era mas el duelo de la prensa que lo que realmente se hacia", afirma. La historia de PUA terminó en 1991, cuando el Doctor Trucho se fue a estudiar a los Estados Unidos. El único que de vez en cuando despunta el vicio es El Chacal, quien se convirtió en un referente obligado para la prensa cada vez que se quiere hablar de hackers. PUA nunca fue disuelta oficialmente.

La Buena Fe de la Red

Ademas del caso Delphi hubo otros que, si bien no llegaron a las páginas de diarios y revistas, tuvieron amplia difusión en el mundillo de los hackers. "Yo tuve uno o dos problemas con mis propias claves de Dialog -recuerda Armando Parolari-; posiblemente en el momento en que hacía las demostraciones alguien llegó a ver la password y comenzó a usarla. Tuve que pedir que me la cancelaran. Eso sucede. Y no hubo manera de saber quién fue." Otra posibilidad es que hayan hecho shoulder surfing: mirar por sobre el hombro de quien tipea y ver qué teclas oprime, así, aunque la clave no salga por la pantalla, se la puede leer y anotar. -La gente que tenía problemas con la facturación recurría a la Justicia -continúa

Parolari-, pero nunca se llegó a nada, a pesar de los esfuerzos. Estuve varias veces en los tribunales colaborando con las investigaciones. Es interesante porque no quedan rastros, es casi imposible identificar al que usa la cuenta. Algunas veces demorábamos la denuncia mientras intentábamos encontrarlos, pero es muy difícil porque se usa una línea telefónica: uno puede determinar que se esta usando una cuenta en forma ilegal, pero ¿quién y desde dónde?

- ¿La policía tampoco podía identificarlos?

- En los casos en los que intervenía la policía se investigaba mucho: un grupo especial de informática pedía la facturación, el listado de llamadas... Les dábamos toda la información que teníamos pero nunca pudieron llegar a algo. Las facturas demoraban tres o cuatro meses y los hackers lo sabían, entonces usaban una cuenta durante ese tiempo y después cambiaban.

- ¿Se podían cambiar las claves en ARPAC?

- ¿Cómo? ¿Cambiar la password? No, no. En ese momento no era posible por un problema tecnológico, la red no admitía... Podía darse de baja, pero como la facturación se hacia en forma manual demoraba cuatro meses.

- ¿Las facturas se cobraban igual?

- Una red no se prepara para la mala fe; en general, el mundo no es así. La Argentina en este aspecto es un país especial. Es muy probable que una red importante, norteamericana, descuente la factura si alguien presenta reclamos. Son políticas de tipo comercial. El riesgo aquí era que, si le descontaban a alguien, todo el mundo iba a pedir lo mismo, nadie iba a aceptar que el gasto era real. Son distintas políticas. En ARPAC no se descontaban.

- ¿No se incremento la seguridad?

- En ARPAC, especialmente, existían condiciones de seguridad muy importantes. Hubo muy pocos casos. En CIBA se dió mas porque la usaban agencias de turismo, bancos... era muy particular. No sé cómo trascendían las claves: podría ser a través del técnico que arreglaba la computadora y revisaba todo lo que tenía... Había gente que lo hacia de forma inocente; ponía la password en la computadora, o le pedían al técnico que la probara porque no podían entrar.

- ¿Cómo se manejaban las passwords?

- Con mucha prudencia. Todos conocían los riesgos. Tal es así que las claves no pasaban por la oficina comercial, iban directamente al lugar donde se las habilitaba. Y la confirmación se hacía telefónicamente, no se dejaba registro de ningún dato para cuidar al máximo la seguridad. La conclusión a la que llegué después de todas esas investigaciones es que alguien les daba acceso a la clave; no había otra manera. En los últimos años me llegaron versiones, que no pude comprobar técnicamente; decían que los hackers habían conseguido un programa que interrogaba a cada computadora y podía llegar a sacar las contraseñas de la memoria. Para mí no es posible, pero en una de esas entran. En las películas es así, ¿no?

¿De donde salían las claves? ¿Siempre eran descuidos de los usuarios, como en el caso de Alejandra? Algunos hackers dicen que la respuesta estaba en ARPAC. El Capitan Piluso -técnico que devino

hacker- comenzó a trabajar en la telefónica estatal a principios de la década del 80 y seis años mas tarde lo derivaron al servicio de mantenimiento de ARPAC. "Cuando trabajás en una red de transmisión de datos tenés la posibilidad de ver muchas cosas sobre la seguridad de los sistemas, porque controlás las comunicaciones. Es parte de tu trabajo", define.

- ¿Es cierto que para cambiar una clave había que esperar cuatro meses?

- ¿Cuatro meses? ¿Para qué? La clave se daba de baja en minutos: el que estaba a cargo del sistema recibía la orden y con una instrucción la anulaba. Es mas... hasta se cambiaba por teléfono, si había dudas. Las empresas se comunicaban directamente con nuestro jefe y él decidía darla de baja o cambiarla, en cuestión de minutos.

- Parolari le dijo a Alejandra que habia un problema técnico...

- No era un problema técnico; era un problema de negligencia, de burocracia, o vaya uno a saber qué. No había impedimento técnico para resolverlo. Parolari no tiene ni idea de como funcionaba la red.

- ¿Que veías cuando controlabas las comunicaciones?

- Yo estaba en mantenimiento. A veces teníamos que probar las lineas, poníamos equipos que se llaman analizadores de protocolo, que permiten ver en pantalla todo lo que pasa en la conexión, incluídas las claves. Cualquiera de nosotros desde una central podía hacer listados con los abonados NUI, que después terminaron circulando por Buenos Aires. Todo el mundo se metía en los usuarios y les cargaba las cuentas...

- ¿Todo el mundo?

- Y, si, cualquiera. El encargado de las NUI se ocupaba de las altas y bajas de las claves de los usuarios. Era un trabajo administrativo, no operaba con la central de ARPAC. Sacaba listados y, si se los pedías, te los daba, así que no era ningún secreto... Era un traficante conocido. Pero no lo hacía con un fin comercial: era por amor al arte, le apasionaba el tema. Si alguien le comentaba que tenía una clave para acceder a algún lado, él decía "¡Uy! Me interesa". "¿Y vos qué tenés para darme?", le pedían; "Yo tengo unos NUI". Y sacaba la lista. Los listados eran parte del trabajo de ese encargado. Una vez por semana el centro de cómputos administrativo de ARPAC emitía un detalle de usuarios con altas y bajas: una copia iba al área de mantenimiento y reemplazaba al viejo. ¿Dónde iba a parar ese viejo listado? El que quería se lo llevaba, algunos lo usaban como papel borrador. El Capitán recuerda que uno de sus jefes, el ingeniero Ramírez -quien ahora trabaja en Startel, empresa que adquirió los derechos sobre ARPAC- llego una mañana, furioso, con un pedazo de listado que había encontrado en un cesto de basura de la calle Florida. También rememora el ultima día laborable de 1988: Canal 13 filmaba frente al Edificio de la República como los empleados lanzaban papelitos por las ventanas. En la grabación del noticiero se veía a la perfección a la gente del noveno piso, la central de ARPAC: tiraban listados de usuarios y claves.

De acuerdo con un estudio casero del Capitán Piluso sobre la lógica de las passwords, en el noventa por ciento de los casos se asocian con algo de la vida del titular: algunas fechas:, el numero de patente, el de registro. Hay algo en la vida de las personas que tiene que ver con la clave de acceso: el nombre de

la perra ("¿Quién sabe como se llama mi perra?", especulan), la fecha en que nació la hija o el nombre de pila.

- Muchos cometen ese gran error -asegura Piluso- porque piensan que hay miles de nombres, pero no son miles; es mas, cualquier hacker tiene cargados en su computadora todos los nombres masculinos, femeninos, de animales, sinónimos. Hay otros que son muy tontos: por ejemplo, en Coca-Cola la clave era "Coke", lo primero que a cualquiera se le ocurre probar. Algunas cosas las encontrábamos y otras eran fallas de seguridad.

- ¿No era habitual que se cuidara la seguridad?

- Había otros temas mas esenciales para resolver que no pasaban por la seguridad, como que la red funcionara bien alguna vez. Había interrupciones del servicio de una a dos horas diarias. Imaginate un banco que pierda contacto con la central durante media hora!

- ¿Por qué pasaba?

- Los equipos estaban pensados para ser usados en lineas telefónicas normalizadas, y aquí ninguna cumplía con las normas de nada. Los cables eran del año de Ñaupa, estaban para tirarlos.

De tanto ver pasar las claves por delante de sus ojos, el Capitán decidió probar alguna e investigar que pasaba en otros lugares. Recuerda un caso especial: la empresa Proceda, que se ocupa de todos los trabajos de informática para el grupo Bunge & Born.

- Nunca me voy a olvidar, porque ahí comenzó mi alias. En realidad había entrado para mirar -cuenta-, pero en ese momento la persona que se ocupaba del mantenimiento se conectó conmigo y me pidió que me identificara. Lo primero que se me ocurrió decirle fue "Capitán Piluso" [N. personaje del capocómico Alberto Olmedo]. El tipo se volvió loco, me decía que estaba burlando la seguridad y que podía detectarme desde la central. Entonces le contesté: "Hay una diferencia. Yo se quien sos vos y vos no sabes quien soy yo". Era un desafío.

- ¿Te detectaron?

- Si. Me desconectaron el módem de entrada. Pero a los diez minutos entre por otra línea. Así hasta que, de tanto joder, descubrieron la clave que usaba y la anularon. Un mes después volví a ingresar con otra contraseña y de nuevo me preguntaron quien era. Dije "de vuelta el Capitán Piluso, ahora con otra password". El tipo estaba a punto de agarrarse un ataque, no lo podía creer; tenían contratado un servicio de acceso restringido a un grupo cerrado de usuarios.

El ingeniero Carlos Manuel Ramírez trabajo durante años en ARPAC en diversas áreas, incluida la de mantenimiento. Ahora continua su labor en Startel. Afirma que "nunca, ni en la época de ENTel, se hicieron listados con claves. Había mucha seguridad". Pero luego medita:

- Es posible que se hicieran algunos listados de clientes con las NUI -acepta-, pero eso era como mi guía interna de clientes. De lo que sí estoy totalmente seguro (porque eso no quedaba registrado) es que desde la propia memoria del equipo de red (que es el único lugar donde se recibe la password) era imposible escribir ese listado.

- Un listado de NUIs contiene teléfonos ¿No es el primer paso para averiguar una clave?

- Es tener el teléfono, es robar una línea telefónica porque se sabe que acá hay una línea de datos, una máquina conectada. Las seguridades eran muy altas en la época de ENTel y son más ahora, que se instaló nuevo hardware y software. ¿Quien podía tener los conocimientos para poder entrar a mirar eso?

- ¿Los que hacen el soporte técnico?

- Los técnicos que operan los centros tienen un altísimo grado de capacitación, pero están orientados para operar y mantener primariamente: saber interpretar las alarmas que salen del sistema y, en función de eso, intervenir cambiando partes. No es gente que esté para meterse en los programas, modificar instrucciones o investigar y acceder a zonas de memoria donde puede estar cargada determinada información. La gente que tiene esa capacitación, básicamente, es la que esta en ingeniería, gente que conoce mucho mas la parte técnica de los equipos en detalle.

- ¿Y los empleados que tipean las claves?

- Y... eso sí. Nadie lo niega. Pero la información no estaba dispersa: la manejaba una sola persona cuando era ENTel. Ahora sigue igual: hay una única persona que tiene las herramientas y los mecanismos para cargar por primera vez las claves en el sistema.

- Entonces la seguridad estaba controlada desde el inicio.

- Bueno, no. En 1982, 1983, cuando arrancó el servicio, había desprolijidades administrativas gordas, que fueron rápidamente detectadas y cortadas. Venia un cliente a pedir una password y se escribía en un papelito: era un trámite administrativo mas, un formulario que se llenaba y circulaba por toda la oficina!

- ¿Cómo llegaba la password al cliente?

- Se la enviaban en un sobre cerrado. Después se hizo un papel con un lado oscuro para que no se pudiera leer a trasluz. Pero en el comienzo, fue de terror.

La Pesquisa de las Claves

De aquellos tiempos se acuerdan Sticky y Truchex. Sticky comenzó -como casi todos en Buenos Aires- con algunas claves de CIBA, pero no pasó mucho tiempo sin obtener NUIs de ARPAC. Cuenta que los hackers mas avezados derivaban a los novatos hacia Altos, Alemania, cuando querían averiguar de donde llamaban, y una vez allí accionaban un comando que descubría nombre, procedencia y NUI (sin la password, obviamente); si el prefijo era 7220 o 7221 se trataba de un argentino. "Para que no pudieran rastrearnos pasábamos por computadoras de distintos países, llamadas PADs, que permitían salir de la red y volver a entrar", explica Sticky, y exhibe unos papeles: "Acá están las PADs de Francia, Inglaterra, Taiwán... Acá esta la de Timenet para Francia. Ahí había un programa trampa para sacar información que puso un amigo mio. Le decía a todo el mundo 'Miren cómo se puede saltar a tal lado' y los flacos se mandaban. Cuando pasaba una comunicación por ahí, el programa se robaba el NUA de destino. ¡Cómo compilaba información!." En esa época no era muy conocido el hacking y los

instaladores olvidaban borrar las cuentas default (por defecto) que trae el sistema original para mantenimiento. Aprovechando ese descuido, Sticky ingresaba en cuanto sistema se le cruzaba en el camino y, entre otras cosas, averiguaba outdials.

- En Altos te daban algunos -recuerda-, pero después se descubrió cómo era el outdial: es el código de zona y un numero. Entonces apareció el programa que servía para escanear los números y evitar que ARPAC te cortara.

- ¿Que conseguiste en Altos?

- Esta -saca otra anotación- era la NASA: con "guest", entrábamos. Una vez entré a la Agencia Especial Europea para ver qué era: los del Chaos la habían hecho pelota, tenías cualquier cosa a tu disposición ahí adentro. Era demasiado grande para mí, no quise ir en cana. Por las dudas... Tengo muchas cosas apuntadas... Del dicho al hecho, Sticky da vuelta cajones repletos de notas y, a medida que los mira, detalla: "PAD de ENTel con ARPAC; Sudafrica, acá también estaba lleno de atorrantes; el Banco de Tokio; una lista de posibilidades que hice cuando le cambiaron la password a FATE. Este es el menú principal de Charlie ¿Les hablaron de Charlie? era un BBS que te pedía sólo el numero de teléfono; yo entraba y hacía un listado de todos los tipos que se habían conectado para conseguir los números. Conozco una chica que cambió el teléfono porque la volvían loca con los llamados...".

La lista continúa por minutos, hasta que encuentra varios papeles de passwords acordadas.

- Son todas truchas -dice Sticky al mostrarlas-, ya no sirven. Las usábamos para entrar a Compuserve. ¡Si les habré pasado los números a varios amigos...! En esa época me llegaban boletines de tarjetas de crédito vencidas y sacaba los datos de ahí.

Sticky se refiere al carding, el arte de abusar de tarjetas de crédito ajenas. El fin mas común del carding era abrir cuentas en sistemas en línea de los Estados Unidos, como Compuserve. Originalmente, teniendo un listado de tarjetas de crédito canceladas, de los que se encuentran en cualquier banco, era facilísimo lograrlo. Cuando el sistema preguntaba el nombre, la dirección y demás datos, se brindaba información falsa; cuando pedía la tarjeta de crédito, se ponía el numero de una cancelada. Como no validaban en el momento, la cuenta se abría con una password provisoria y podía durar una o dos semanas, hasta que llegara -mas bien, no llegara- la confirmación.

- ¿Nunca los descubrieron?

- ¿Quien corno, en esa época, iba a venir a la Argentina para averiguar quién estaba haciendo cuentas truchas? Se pudrió cuando Compuserve llegó al país. Los tipos se cansaron de que los truchearan. Las cuentas duraban unos doce días y, mientras tanto, tenías acceso a casi todo, excepto cosas muy importantes. Como no daban mucha bolilla hacíamos de todo. ¡Hasta entramos a la máquina de reserva de los vuelos!: podíamos conseguir pasajes para cualquier lado.

Adam, el de las pinchaduras telefónicas, también conocía los principios del carding y las posibilidades de acceder a las reservas de vuelos. Una vez, en Miami, reservó un pasaje aéreo vía Compuserve y lo pago con una tarjeta de crédito. Lo único que tenía de la tarjeta era el cupón que un usuario descuidado se había olvidado en una estación de servicio. El pasaje lo usó una señorita en apuros que debía alejarse

con urgencia de La Florida. Se rumorea que un hacker local, hoy importante empresario de telecomunicaciones generó medio centenar de cuentas mediante carding y las vendió en una reunión de usuarios de un BBS. Ofrecía un paquete completo: NUI de Arpac, NUA de Compuserve y clave de acceso, más las instrucciones, al módico precio de cincuenta dólares. Fue demasiado: al poco tiempo Compuserve cambio el método de validación y el truco se volvió imposible. Los hackers, sin embargo, no se dieron por vencidos. Descubrieron que se podía engañar de la misma manera a PC MAGnet, red de PC Magazine. Nada muy interesante, pero tenía acceso a Compuserve y, como este suponía que PC MAGnet validaba correctamente a sus usuarios, los aceptaba sin excepción. Compuserve, junto con The Source, fueron fuente de novedades de software para los hackers; luego se agrego Channel 1, BBS norteamericano, uno de los más grandes del mundo. Algunos hackers tenían cuentas legales en esos servicios, pero usaban claves ajenas de ARPAC para acceder a ellos.

Truchex hizo su fama por disponer siempre de passwords: si no había ninguna dando vueltas, el tenía una para compartir con sus amigos. Cada vez que una contraseña dejaba de funcionar, los hackers que querían entrar en algún BBS de Estados Unidos no dudaban: "Preguntémosle a Truchex".

- ¿De dónde sacabas las claves de ARPAC?

- Surgían de algún disidente arpaquiano -cuenta-. Había uno adentro que las vendía: las cobraba dos mil dólares! Me pasó información interesante sobre redes, como manuales de X.25, que en ese momento no estaban a disposición de todo el mundo. Pero yo jamás compré una clave. Él me decía "ya te voy a entregar"; podía esperar años: nunca lo hacía. Después cambiaron el sistema de passwords y quedó muy caliente porque el arsenal que tenía, su tesoro, dejó de tener valor.

- ¿Y cómo las conseguías?

- De las formas más diversas: en las mensajerías locales, o por comunicaciones telefónicas anónimas, o a través de los grupos de usuarios de phreaking y hacking internacionales que, a veces, me daban claves argentinas confirmadas en QSD... Eran de orígenes diversos. Me acuerdo de un tipo que hacía mantenimiento de máquinas y proveía muchísimas passwords.

Para llegar a ser un especialista en claves de ARPAC, Truchex tuvo que recorrer un largo camino. En 1987, con dieciocho años, llegó a sus manos el dato de una cuenta Delphi con salida a Estados Unidos cuya contraseña era igual a la password. Gracias a un concurso de juegos se conectó, desde el primer ingreso y a través de los mensajes privados, con la peruana Playgirl, su cicerone en los caminos hacia la red francesa QSD. A través de Delphi no tenía forma de acceder, de modo que preguntó y consiguió una clave en CIBA. Sin entender lo que hacía, siguió las instrucciones hasta llegar a QSD y convertirse, según calcula, en uno de los primeros argentinos por aquellas tierras. Allí se inició en los misterios del phreaking con un grupo de alemanes que organizaban teleconferencias. El principal coordinador era Mike, de Düsseldorf, fundador del PHI, Phreakers International. Mike organizaba las conferencias telefónicas que admitían un máximo de sesenta y cuatro personas en línea, aunque no todas a la vez.

"En esas reuniones había de todo -comenta Truchex-, hasta gente que pedía drogas porque, dados los precios en Alemania, las podían colocar muy bien, y un pirata del video que ofrecía Roger Rabbit cuando todavía no se había estrenado en Estados Unidos." Una teleconferencia en particular duró casi seis horas. Esa vez llamaron a Mario Vargas Llosa a Perú para hacerle una entrevista muy seria sobre su

candidatura a presidente, para una revista internacional. La operadora interrumpió la charla para decir que habían superado el crédito establecido para conferencias y que necesitaba hablar con el titular de la calling card. "El alemán -evoca-, fresco como una lechuga, le contestó que el señor Johnson, titular de la línea, festejaba en Acapulco el éxito de su fábrica de jabón, pero que en ese momento estaba comunicado a través de una terminal y le confirmaba que podía usar el servicio hasta cubrir cinco mil dólares. La operadora mucho no le creyó, pero nos dejó media hora mas y cortó."

Truchex sostiene que QSD "siempre fue un curro muy grande de Erik, el operador. Cobraba comisiones por las líneas que mantenía ocupadas de la red francesa Teletel. Era absolutamente consciente de que todos los usuarios eran piratas que usaban accesos ilegales, pero lo favorecía. Tenía horas pico en que estaba bloqueado, por la cantidad de gente conectada. Hoy en día está vacío. Las últimas veces que ingresé era el único usuario". Allí conocio a Skeadrow, The Operator, Par y Gandalf -entre otros-; muchos de ellos cayeron en distintos operativos, como Sundevil. "Los secuestraron de sus casas, los incomunicaron de sus familias. Los soltaron después de tres meses y largas negociaciones -recuerda-, pero nunca más volvieron a pisar el terreno de las telefónicas. Nadie lo podía creer, pero era cierto."

Truchex y sus amigos se divirtieron recorriendo el mundo a través de las lineas informáticas y gracias a las PADs. Ingresaban en una máquina por una línea y salían por otra, para conectarse con una segunda computadora y así seguir, hasta pasar por Sudáfrica, India, Singapur, Canadá, Inglaterra y volver a Buenos Aires. Todos los sistemas estaban montados sobre VAX, un modelo de computadora de la Digital Equipment; tenía un agujero en la seguridad que permitía el ingreso de hackers en los centros de datos más importantes del mundo. Truchex compró su computadora en 1986; antes, hackeaba con el ordenador de un amigo. En esa casa conoció a Alex, poseedor de valiosa información que entregaba a cuentagotas y gracias a quien obtuvieron la clave "FASAGRA" de la cuenta FATE. En esa época frecuentaban los BBSs Norad y Charly, prácticamente lo único que había por conocer en la Argentina. Para comunicarse con los Estados Unidos utilizaban, por supuesto, outdials.

- La primera lista la conseguí antes de que la publicaran en PHRACK, por un tipo que tenía una amiga que trabajaba en Telenet. Era muy piola porque se podía hacer desde casi todas las ciudades, aunque con la telefonía de aquí la máxima velocidad que logramos fue 1200 Baudios. Después estaban los outdials globales: muchos estaban mal configurados y les podías pedir una linea a través de AT&T poniendo el prefijo 10-2-88. Esto era un secreto máximo -confía-, no lo sabía nadie.

De esa manera ingresaban en PC Pursuit y, a pesar de la lentitud en la comunicación lo utilizaban para sus recorridas. Ademas del detalle de Truchex, otros testimonios dicen que las claves de ARPAC se conseguían por ingeniería social.

- Buenas tardes, lo llamo de ARPAC. ¿Tuvo problemas con su cuenta últimamente?

La respuesta era obvia, ya que la red nunca funcionaba bien.

- Sí, el otro día trate de acceder y me decía CLR NC y un numero.

- ¡Otro caso! Exactamente lo que suponíamos. El problema es que se borraron algunas claves de nuestra máquina, por eso las estamos ingresando a mano. ¿Puede darnos su contraseña, así hacemos lo mismo?

- Si, cómo no... N91...

El usuario confiaba en una voz en el teléfono y daba su password. Si hubiese leído el manual que le entregaron con su cuenta, aún esa hoja mecanografiada, hubiera sabido que CLR NC significaba que la red estaba congestionada y era imposible establecer una comunicación en ese momento. De esa manera muchas empresas perdieron claves. Un hacker hizo este trabajo para tener una cuenta exclusiva que le durara mucho tiempo. Pero se la pasó confiadamente a un hacker mexicano que tenía muchos amigos en Buenos Aires. Al poco tiempo circulaba entre por lo menos diez personas y la empresa en cuestión tuvo que pagar una cuenta de veinte mil dólares. Pero eso fue en los últimos años de ENTel. En los tiempos dorados, cuando las claves duraban meses gracias a la ineficiencia de la telefónica estatal, las NUIs robadas circulaban con absoluta libertad. Los que se comunicaban con cierto BBS se reunían periódicamente para intercambiar software, pirateado o de dominio público. En una de esas reuniones estaba Alejandra, quien junto al dueño de casa llamo a Truchex para conseguir una NUI. Ni bien cortaron dijeron a las treinta o cuarenta personas presentes: "Anoten: N91..." En ese momento se desató una lucha por el lápiz y el papel para anotar el numero mágico que les permitiría llamar gratis a todos lados. Una de las claves, conseguida por un peruano, duro prácticamente un año y la usaba todo el mundo. Pocos días después de que dejo de funcionar, en una reunión de piratas, Der Katz se presentó con un cartel: "Adiós A123Z". Fue la despedida. Otras maneras de conseguir NUIs era engañar a algún hacker. Doctor Trucho convenció a un colega de que le prestara su clave para llamar a cierto lugar.

- Okay, pero te conecto desde mi casa y tipeo la clave yo, porque si la ves me la vas a robar- sospechó el amigo.

- ¡Pero, che! Me parece de mal gusto que desconfíes así. En fin, para que veas que no hay ningún problema, hagámoslo a tu modo. Lo único que te pido es que usemos una línea que conozco, que tiene menos ruidos. Como vos no me das tu clave, yo llamo a ARPAC y, una vez conectados, te dejo operar a vos.

- Hecho.

El número al que llamó Doctor Trucho era la casa de El Chacal, quien estaba esperando con un módem y un programita que emulaba ARPAC. Se conectaron, el incauto tipeo la clave, El Chacal la guardó en un archivo de su computadora y devolvió un CLR NC.

- Esta congestionado. Probemos otro día- propuso Doctor Trucho.

- Bueno, no hay problema.

El Doctor nunca volvió. La demanda de passwords nuevas era tal que dos hackers diseñaron un virus informático especializado en capturar NUIs. Su misión era copiarse en toda máquina que pudiese y esperar que se tecleara "N91". Guardaba las teclas en su propio código y se reproducía con esa

información adentro. La esperanza de estos hackers era encontrarse en algún lugar con una copia del virus que tuviera una NUI nueva. Pero nunca lo probaron, a pesar de que parecía buena idea.

La época del hacking indiscriminado a ARPAC terminó unos dos años después de su privatización, cuando agregaron la posibilidad de consultar las llamadas realizadas y cambiar la password en linea y sin demoras. Eso demuestra que la causa de los problemas de ARPAC era el manejo ineficiente de las claves, que permitía que se siguieran usando durante meses después de robadas, e incluso denunciadas. Otra causa de la decadencia fue la velocidad de comunicación: 1200 BPS hasta 1993 (luego subió a 2400), mientras que una técnica antigua en los Estados Unidos, y novedosa en la Argentina, permitía usar toda la capacidad de los nuevos módems de 14.400 BPS: la Blue Box (caja azul).

V. Jóven (Hacker) Argentino

"Para los argentinos la libertad es algo que no se toma a la ligera. No fue hace mucho que los jóvenes que se manifestaban contra el gobierno (militar) o hacían algo que la Junta consideraba inaceptable simplemente desaparecían sin que se volviera a saber de ellos nunca más. La gente que entiende la tecnología y tiene la voluntad de aprovecharla en beneficio de una mayor libertad individual siempre va a encabezar la lista de enemigos de un régimen represivo. No podemos cerrar los ojos ante este hecho ni engañarnos pensando que estamos a salvo de esas fuerzas malignas."

EMMANUEL GOLDSTEIN, "INSPIRACION", EN 2600

(VOLUMEN ONCE, NUMERO CUATRO)

Cajitas de Colores

En 1992 muchos usuarios de diversos países comenzaron a conectarse con algunos BBSs underground de Buenos Aires. Alemania y los Estados Unidos eran los orígenes mas frecuentes, pero todos tenían dos cosas en común: usaban computadoras Commodore Amiga y llamaban a través de la *Blue Box*.

Los hackers locales no tardaron en averiguar el modo en que llamaban y empezaron a hacer preguntas. Poco a poco juntaron la información necesaria como para practicar Blue Boxing por su cuenta: a qué números llamar, qué frecuencias usar, cómo hacerlo. Esta actividad -vieja en los Estados Unidos, casi en desuso por los controles y la legislación en su contra- empezó en Argentina en los 90, gracias a los avances tecnológicos. Hasta esos años la mayoría de las centrales telefónicas eran mecánicas o electromecánicas y no había modo de llamar al exterior directamente. En esas condiciones, la Blue Box era imposible, solo se podía intentar la *Black Box*. La instalación de lineas telefónicas con DDI y centrales digitales permitió que las cajas azules llegaran a la Argentina y se expandieran. A pesar de tener todos los elementos técnicos, un obstáculo detenía a los hackers argentinos: sus colegas extranjeros hacían Blue Boxing con programas para Amiga y los locales no tenían una. Las opciones eran construir una Blue Box por hardware (el clásico aparatito que se usaba en los 60) o conseguir algún programa que funcionara en PC, usando una placa de sonido para emitir los tonos adecuados de acuerdo con la tecla que se pulsara. Como nadie tenía ganas o conocimientos como para hacer lo

primero, se dedicaron a la segunda opción. Al fin llegó un programa para PC: el Omega Box. De origen italiano, se podía configurar para abusar con tranquilidad de la empresa telefónica que se eligiera.

Comenzaron con los códigos de France Telecom: llamaban a un numero gratuito en Francia, cuyo uso normal era para cobro revertido, y una vez conectados tomaban el control de la comunicación con la Blue Box, que les permitía llamar prácticamente a todo el mundo. Cuando las compañías cambiaban sus códigos, probaban con otras: Telefónica de España, la norteamericana MCI, la Telefónica de Chile o Australia.

- Che, Joe, decime una cosa ¿cómo se usa este programa? Estoy escuchando los ruiditos, que son muy flasheros pero no me dicen mucho -preguntó Alan Turing.

- Es fácil. Mirá: con Q das el hang-up (señal para que corte el teléfono); con W, el pedido de línea; con D, el teléfono. Con T das el hang-up y pedido de linea con los tiempos que requiere Telecom France -contestó Joe Montana.

- Pero la secuencia, entonces, ¿cómo es? ¿Pongo el teléfono al lado del parlantito?

- Llamás al 00-33-800-999-111. Cuando te atiende el operador, le mandás Q hasta que escuches un pitido chiquito detrás. Obviamente, ahí tenes que acercar el fono al parlante, o el parlante al fono. Después dale T, así te manda con los espacios reglamentarios. Ahí le das el D para que disque y... voilà!

- Okay. Voy a ver que tal anda. ¿Vos cómo tenes conectada la placa de sonido?

- Directamente.

- ¿Con qué salida? Porque es estéreo...

- Ni idea, la mía es mono. Pero ojo, que manda los mismos tonos por los dos canales!

- Ah, joya. ¿Y el tema de las compañías, ¿como es? ¿Tengo que seleccionar Francia? ¿O cualquiera?

- No, no: sólo Francia.

- Otra cosa. Cuando vos llamabas a Estados Unidos, ¿ponías 10 en vez de 1?

- Es así: primero ponés B y el código del país, en ese caso 1; después ponés 0 (eso significa maxima prioridad en el satelite) y mandas el código con el de larga distancia incluido.

- ¿Cómo, cómo? Dame un ejemplo.

- B490896017504C. Eso es Múnich. Código de Alemania, 49; código de la ciudad, 89. El resto es el número de teléfono. Al final hay que poner C.

El diálogo surge de la memoria de Alan Turing, quien además recuerda la fascinación que ejercía el Blue Boxing en quienes lo practicaban: "Uno llamaba a MCI y la operadora preguntaba 'May I help you?' ('¿Puedo ayudarlo?'). La tentación era decirle: 'Yes. Please, hang up' ('Si. Por favor, cuelgue')". La primera orden que se le daba a la central desde la Blue Box para tomar control de la línea era "hang-up"; no hacia falta decir nada: de eso se encargaban los tonos. "En Telecom atendían con una musiquita; cuando hablaba el operador le daban los comandos y ni se enteraba -afirma Turing-, siempre que uno lo hiciera bien. Me contó Joe Montana que una vez las cosas fueron mal y el operador de

Francia empezó a putearlo, en castellano y frances. Los tipos ya sabían lo que estaba pasando y no podían evitarlo."A diferencia de los hackers norteamericanos mas famosos, exploradores del sistema telefónico como Cap' Crunch, los argentinos usaban la Blue Box para motivos mas prosaicos: básicamente, para llamar a amigos en el exterior. Doctor Trucho, que estaba estudiando en los Estados Unidos, era uno de los blancos favoritos. Si no estaba le dejaban mensajes en el contestador, donde atendía la voz de algún dibujo animado, en ingles. Cuando llamaban a alguien sin explicarle el método que utilizaban, el receptor se ponía nervioso y hablaba rápido, pensando que el interlocutor gastaba fortunas. Cuenta Alan: "Me paso con la madre de un amigo en España. Mi amigo se había mudado y ella quería explicarme que no tenía teléfono en la casa nueva. Se ponía nerviosa porque yo no tenía ningún apuro en cortar y le preguntaba cosas de su hijo". Además del Doctor Trucho, Alan hablaba con otro amigo, que vivía en la costa Este de los Estados Unidos. Lo llamaba al trabajo y conversaban hasta que los jefes del amigo le pedían que cortara y se pusiera a trabajar. Joe Montana tiene experiencias similares.

- Llamaba al Doctor Trucho para charlar -cuenta- y a BBSs concretos para investigar software. Traje programas europeos que acá no se conocían y fueron un éxito. Llamaba sobre todo a BBSs alemanes, donde hice bastantes amigos. Había una pareja de granjeros, muy copados los dos, que tenia un BBS con dos nodos en una granja de leche. Me quedaba horas charlando de la vida, pasándonos cosas...

- ¿Como hablaban?

- En general todas esas comunicaciones eran por módem; pocas veces me comunique personalmente con alguien. Sobre todo porque me resultaba mas fácil leer y escribir en inglés que escuchar y hablar. No todos llamaban a amigos. Algunos encontraron la veta comercial y usaban la Blue Box para llamar a BBSs piratas de los Estados Unidos y Europa, donde encontraban los programas mas recientes o las novedades en juegos. Algunos los vendían en casas de computación y sacaban enormes ganancias; otros los copiaban en sus BBSs y cobraban el acceso. El negocio prometía y los hackers pasaban el día pirateando; algunos compraron una línea telefónica exclusivamente para hacer Blue Boxing. Pero tanto va el cántaro a la fuente...

- A veces los muchachos de telefónica me descolgaban cuando estaba haciendo Blue Boxing -confiesa Metallica.

- ¿Por qué? ¿Te detectaban?

- Me engancharon mas de una vez. Recuerdo estar hablando con el Doctor Trucho y de repente escuchar ruidos en castellano. No solamente en castellano: en argentino. Ruidos de pasos, música como de una radio puesta de fondo... Ahí nomas corté. A los treinta segundos levanté el tubo y seguía escuchando el mismo ruido. Volví a cortar.

- ¿Tuviste algún problema?

- Nunca. No llegó nada, ni la cuenta de las llamadas al exterior. Pero el cagazo que me pegué fue terrible. Después de eso no hice mas Blue Boxing por dos o tres meses, hasta confirmar que estaba todo bien. Alguna gente recibió cuentas astronómicas de teléfono...

- ¿Quiénes?

- Un negocio que vendía jueguitos y que había comprado una línea para hacer Blue Boxing. Estuvo colgado no sé cuantas horas y le llegó una cuenta de veinte o treinta mil dólares. Imagino que vieron que llamaba demasiado afuera y lo monitorearon. Se dieron cuenta de que usaba siempre cobro revertido y Telintar estaba pagando por eso, entonces se lo facturaron. Pero me parece que hicieron una facturación selectiva, porque yo usé la caja un par de veces y no pasó nada. Si la usabas como si estuvieses pagando, digamos quince o veinte minutos una vez por semana, no pasaba nada.

Joe Montana, después de haber hecho Blue Boxing durante años, formó su opinión sobre el hacking y el phreaking:

- Todo tiene limites. Si uno tiene un cierto criterio de realidad, sabe que hay distintas etapas. Al principio hacés ARPAC: jugás un ratito, es fácil, no requiere demasiada inteligencia. La siguiente etapa es la Blue Box; la siguiente, el hacking. Yo ahí ya no me metí: tenés que hacer cosas mucho mas complicadas y que requieren poca ética, o que tu ética este más allá que eso. Para mí lo importante de la investigación -que era entender cómo funcionaban las redes telefónicas- ya había terminado. Logrado eso, no había mas nada que hacer. Lo siguiente era investigar sistemas grandes, y eso significaba hackearlos. Ahí hay un tema de ética que nunca terminé de resolver. No si estaba bien o mal, sino si yo debía o no debía hacerlo.

- ¿Por qué?

- Porque me parece que no me correspondía a mí como usuario de los sistemas en general, probar uno para decir si andaba bien o mal. En definitiva, esa es mi idea de lo que es un hacker. Por un lado, yo nunca me sentí capacitado para hacerlo; por otro, aún en el caso de estar capacitado, me parece que se puede hacer de otra manera, mas directa y menos underground. Es una cuestión de respeto por el otro, que está trabajando, haciendo un sistema. Yo no puedo entrar a una casa rompiendo una puerta.

Joe decidió no comprometerse. Además -argumenta- tenía cosas mas importantes que hacer. Nunca se considero un hacker y cree que del cracking, el phreaking y el hacking, el arte mas noble es el del phreaking. Los otros dos, para él, violan la propiedad intelectual, no respetan el trabajo de la gente que hace cosas porque tiene ganas o porque le pagan.

- Pero el phreaking -aclara- es diferente. Tener respeto por una empresa es otra cosa: una empresa no es una persona y, además, muchas veces se trata de una empresa que cotidianamente nos roba. A mí, por ejemplo, hace quince días que no me anda el teléfono y no me lo solucionan. Ahí sí que no me importa: si puedo recuperar algo de la guita que me roban todos los días, no tengo ningún problema.

Recambio Generacional

De la nueva generación de hackers argentinos, Opii es uno de los más reconocidos, pero se niega incondicionalmente a relatar sus aventuras. "La paranoia tal vez suene exagerada -admite a modo de disculpa-, pero no es así. Tengo muchos amigos que cayeron en las manos del FBI, en Estados Unidos. Les hicieron juicios: algunos fueron a la cárcel, a otros les dieron distintas penas, pero a casi todos les sacaron las computadoras, es decir, todo lo que tenían. Y en general eso pasó porque hablaron de más, porque dijeron 'Yo entré a tal lugar, hice esto o lo otro'. Eso llama la atención, ¿no?. Si bien en la Argentina todavía no hay legislación y el hacking no es tan conocido, yo, por lo menos, no quiero llamar la atención y ser EL hacker. Podrían decir 'Ah, seguro que eso lo hizo Opii." Janx Spirit refuerza

las explicaciones: "Si yo te digo que hackeé la SIDE, que les dí vuelta todo, y lo lee el tipo que era operador de la SIDE, se va a enojar mucho, va a hacer lo imposible para averiguar quién soy y romperme la cabeza, ¿no? Yo no quiero problemas". Opii tiene veintitrés años.

Comenzó su relación con las computadoras a los doce, cuando en su casa compraron una Commodore VIC 20 que le servía para programar en BASIC. Pasó por un modelo 64 y un módem con el cual se comunicaba con sus amigos, hasta que llegó a una vieja PC. "De alguna forma conseguí ciertos números, ciertas claves para entrar a ciertos lugares. Debe haber sido en el '89, cuando CIBA era utilizable. Un día ví unos números en unas carpetas; me fijé que eran y vi cosas extrañas... Me gustó y listo. Después llamé a esos lugares, conocé a otra gente y aprendí un montón", explica Opii, alardeando de lo específico de su confesión.

- Cuándo encontraste esos números, ¿ya sabías para qué servían?

- Tenía una vaga idea: eran para llamar a algún lugar, pero no sabía adónde ni qué había. Y, bueno, probé. Puse la clave, llamé por teléfono y me encontré en un lugar donde había otra gente conectada. Se intercambiaban mensajes. Okay, tengo que admitir que el primer lugar al que ingresé era QSD. Un lugar que, digamos, resulta interesante un par de minutos.

- ¿Te abrió otras puertas?

- Para nada. Sólo me sirvió para saber que había gente en otros lugares, que se podían mandar y recibir mensajes o conversar con personas que no conocía. Me pareció bárbaro, impresionante... Conocí gente que, de otra manera, nunca podría haber conocido. Después siempre traté de aprender cómo funcionaban las cosas que encontraba: un sistema, una máquina... saber que se podía hacer con eso.

Janx Spirit tiene diecinueve años y esta muy preocupado por parecer un chico duro. "Uno de mis hobbies es salir los sábados por la noche a... bueno, digamos a destruír. Nada en particular -precisa, riéndose-: destrucción en general. Cosas divertidas, para pasar el rato. Después, nada: salir, pasarla bien hasta que tenga que pasarla mal". Sobre su metier comienza por señalar que la primera máquina que vio fue una Commodore 16. "Ni bien entró a mi casa salió de una patada. La había comprado mi viejo pero con mis hermanos le dijimos que no, que queríamos una 64. De ahí pasamos a una XT, que me pareció una garcha; entonces me compre una Amiga y un módem de 300 Baudios, con los que conseguí pocas cosas buenas. Recién con la AT y un módem de 1200 empecé a conocer gente, lugares, cosas... De eso hará unos dos, tres o cuatro años... No sé, no me acuerdo con precisión."

- ¿Cómo conociste a Opii?

- Porque una vez el muy infeliz me mandó un mensaje. De entrada le dije que se fuera a la mierda, pero me enteré de que no era un boludo y le contesté un poquito mejor. Entonces empezamos a mandarnos mensajes.

Logical Backdoor, diecinueve años, asiente ante las intervenciones de sus colegas. Se pierde en una delirante explicación sobre el origen de su alias -mezcla puertas traseras, programación en Clipper y las opciones "True" y "False" ("Verdadero" y "Falso")- para desaparecer en beneficio de "otros planes mas interesantes que charlar". Opii y Janx se hacen cargo de una pizza, varias cervezas y las respuestas.

- ¿Son una banda?

- No sé si tanto como una banda. Una jauría, tal vez. Somos un grupo de amigos -sostiene Janx-, no una barra armada. Por ahí hacemos cosas organizadamente, pero de casualidad, porque organizarnos es un trabajo terrible.

- HBO, ¿no es de todos?

- Si, pero la cuestión es que no hace falta un BBS que diga las veinticuatro horas 'Esto es HBO' para tener un lugar donde hacer lo que queremos. No hay grupo. Somos amigos que se reúnen y hacen cosas porque tienen ganas -define Opii.

- No se trata de un grupo que se dedica a hackear organizadamente. Hay cosas que son mas fáciles de hacer con otras personas: lo que uno no sabe o no tiene, el otro si. Eso es todo. Digamos que nos complementamos. -reafirma Janx.

- ¿Qué hicieron juntos?

- En cierto viaje -a cierto lugar de Sudamérica, para ser generoso con los detalles- nos encontramos en el área de embarque y estuvimos a punto de decidir adonde nos íbamos. Alguien se había olvidado de apagar las maquinitas, las dejaron solas y nos pusimos averiguar cómo trabajaban: casi sacamos una password para irnos a cualquier parte del mundo, pero no había vuelo a ningún lugar interesante -evoca Opii y cuando mira a su amigo ríen los dos.

Ambos son de la vieja guardia: aprenden los sistemas, los respetan y no consideran hackers "a los tipos que solo quieren usar algo -hacer llamadas gratis, sacar alguna ventaja-, a los que no les interesa por que o cómo hacen las cosas. Esos se contentan con una clave, la usan hasta que no funciona más y tienen que esperar a que alguien les dé otra", describe con desprecio Opii. Janx completa: "Están los que destruyen cosas, los que disfrutan de entrar a un lugar y borrar todo. Tal vez se sientan poderosos, pero a mí me parece estúpido eso de andar a los hachazos. Están también los que entran a lugares, para sacar información y venderla: desde mi punto de vista, son mercenarios".

- Algunos quieren saber que están haciendo -interrumpe Opii-, cómo funcionan las cosas y qué uso diferente se les puede dar; tratan de investigar lo que encuentran, que por ahí es un sistema o una súper computadora, como la CRAY, procesadora de cuentas corrientes. A mí no me interesan las cuentas corrientes, pero quizá puedo usar la computadora para otra cosa.

- ¿Aprendieron algo hackeando?

- Mucho. De hecho -argumenta Opii- más que en la escuela, la universidad o un curso de cualquier cosa. Por ejemplo, jamás en mi vida fui administrador de una máquina VAX y, sin embargo, puedo manejarla. Jamas en mi vida tuve un UNIX, pero lo conocí tres años antes de que me lo enseñaran en el colegio. El asunto es hacerse preguntas. La red telefónica se usa todos los días, pero nadie sabe qué pasa al marcar los números: la gente sólo entiende que del otro lado suena y alguien contesta. Pero en el medio, ¿qué pasa??; después, ¿qué pasa? A mí me gusta eso. Mentiría si dijera cómo funciona la red telefónica -es muy complicada-, pero algo aprendí.

- El problema es el mito de los hackers como genios -lanza Janx-: eso es mentira.

- Tal cual. En realidad -agrega Opii-, los usuarios son idiotas. Eso es lo que pasa. No necesitas ser un genio: es cuestión de sentido común. Cierta inteligencia, alguna idea, sentido común, y tiempo. Nada mas.

- Janx, antes hablabas de tus hábitos destructivos. ¿También te interesa romper sistemas?

- No, eso es distinto. Destruir es para mi una simple expresión de agresividad, pero cuando le pego a la tecla no le pego a nada. Si rompo algo es físico, como un auto -por ejemplo-, y lo hago caminando por la calle, no adelante de una computadora. Me siento un pobre infeliz si desarrollo violencia detrás de la computadora.

- Claro. Igual que el cybersex -compara Opii-: violencia o sexo a través de la computadora es una estupidez. Si querés eso andá a la calle, a algún lugar. Pero sentarte frente a la pantalla, como un idiota, a escribir "Oh, yes, Marcia! Yes, yes! Oh, oh, ah, ahhh!"…

Para ellos no es difícil conseguir información que les permita incursionar por cualquier empresa: aseguran que con solo husmear en la guía telefónica se puede averiguar las líneas de datos. Un banco local de primer nivel anuncia el número telefónico de su banca electrónica; al discarlo, un módem atiende el llamado y, de allí en adelante, hay que alumbrar alguna idea, o probar. Ninguno de los dos incursionó en los bancos porque no les interesa el dinero, pero saben que en general tienen sus propios sistemas o utilizan mainframes, algo corriente en cualquier lugar del mundo. Para Opii las cosas que se encuentran aquí "son muy aburridas: no hay información jugosa, que te haga cagar de risa".

- ¿Qué es una información jugosa?

- Recuerdo un administrador de un sistema UNIX pirateando software en una red internacional. El tipo -describe Opii- distribuía en una red: la comunicación era por e-mail, se anunciaba "Puse el Corel Draw 5.0 en tal lugar; bajátelo y pasáme éste o el otro". En teoría, no podia estar haciendo estas cosas: supuestamente era el representante de la ley, que siempre causa problemas. Cuento lo que ví en una red internacional. No preguntes más.

- Creo que tenemos un sentido del humor particular. Por ejemplo -se jacta Janx- estás escondido en un lugar y el administrador dice: "Me parece que tenemos hackers", pero se refiere a una cuestión natural, como una mala manipulación del sistema, que puede ser, o dar un O.K. cuando no corresponde. Es divertido verlos hablando sobre los hackers porque el directorio tal se les llenó de basura y resulta que tienen un programa que funciona mal, que cada vez que lo utilizan se les ensucia el directorio.

No es común que algo así pase en el país, comentan, porque hay muy poca gente capacitada para manejar máquinas o redes de computadoras. No es lo mismo una máquina corriendo en DOS que una red de ordenadores con UNIX o VAX con VMS. Según ellos, aquí hay muy poca consciencia sobre la seguridad en sistemas y falta gente capacitada para manejar ese tipo de equipos.

- ¿Alguna vez se encontraron con el operador de un sistema en el momento de hackearlo?

- Hace mucho tiempo. Entre a un sistema -recuerda Janx- y empecé a boludear, a dar vueltas. De repente se me corta. Llamo de nuevo y uso otra cuenta. El tipo pensó que no estaba paseando, que lo estaba jodiendo, y me cambió las passwords; entonces yo, que ya estaba adentro, cambié también las

passwords. Pase diez minutos peleándome con el operador hasta que al final dije basta. Llamé al chabón y le dije: "Su máquina va a ser apagada enseguida. Por favor, corte". La bajó, la prendió enseguida, entré de vuelta y desde el momento en que la apagó no lo vi nunca mas... Me moría de risa, realmente.

- A mí me paso tambien -contesta Opii-, en una máquina de una universidad extranjera. Estaba usando una cuenta cualquiera, una máquina que habían dejado sin password los muy estúpidos: el administrador me mandó un mensaje preguntándome quien era y que hacía ahí, advirtiéndome que esa máquina era solo para uso de los graduados de la universidad. Yo le dije que un amigo me había dicho que podía usarla a través de una cuenta sin password y el me preguntó quien era mi amigo. 'No te puedo decir porque seguro que le vas a hacer algo', le dije; 'No, te prometo que no le hago nada', me contestó. Yo me hacia pasar por mujer y seguí negándole quien era mi amigo e insistiendo en que no hacía nada malo, y el tipo otra vez me preguntó quién me había dado los datos. Le inventé toda una historia y el chabón al final me dio el teléfono de su casa: terminó por darme información cuando en realidad su intención era saber cómo yo había conseguido la puerta para entrar a la universidad. Obviamente, no lo llamé, pero podría haberlo hecho diez días después y decirle: "Habla John Smith, de la Dirección de la Administración del Network Operator Center y necesitamos su clave porque tenemos problemas con el disco de las máquinas tal y tal, hicimos back up y tenemos que restablecer todas las passwords a los que tenían antes...". Con un poco de ingeniería social hubiera conseguido las claves necesarias para ingresar cuantas veces quisiera.

Fieles a la tradición, y como hombres serios que aseguran ser, tratan de no dejar rastros en los sistemas que hackean, o por lo menos lo intentan. No dejan mensajes excepto que entre en confianza con el operador, cosa que se logra mediante la lucha de de uno para ingresar y del otro para evitarlo, o por un largo tiempo de uso.

- ¿Alguna vez no pudieron borrar los rastros?

- Una vez -cuenta Opii-, en un lugar bastante próximo. Entré a través de otro lugar gracias a un usuario que tenía cuentas en los dos y era muy tonto. El tipo tenía un sistema de conexión: desde una máquina podías entrar a la otra sin necesidad de password, porque si era Juan en una también lo era en la otra. Cuando me dí cuenta de que estaba en otro lugar ya era un problema. Eran las cinco de la mañana, mas o menos. Me quede media hora buscando cosas y me fuí a dormir, pensando en seguir otro día. A la tarde siguiente no pude entrar: los tipos se habían dado cuenta.

- A veces merecemos gratitud. Cuando entrás a un sistema y no funciona nada -explica Janx-, si queres usar algo no te queda otra que arreglarlo. Y después hablan del maldito hacker que se aprovecha...

Opii comparte la opinion: "Tenés que arreglar todas las cosas para poder usar el sistema porque está mal configurado, y encima de que lo arreglás dicen 'Ah, está entrando un tipo que usa la máquina, arruina todo, borra archivos'. En realidad, lo que hacés es arreglar lo que ellos hicieron mal, y eso que les pagan para hacer las cosas bien... Son especialmente inútiles en este tipo de cosas, hábiles en hacer todo mal". Trabajo duro y sacrificado el de un hacker. Acuerdan también en que ese tipo de problemas se dan en la Argentina mas que en cualquier otro país del mundo por dos razones: porque las empresas abaratan costos sin medir qué pierden en el camino y porque carecen de parámetros para saber quien sabe y quien no.

Segun Janx, las entrevistas laborales son del tipo "'Pero usted, ¿sabe de esto? A ver, ¿cuánto sabe?' 'Y... mucho.' El que hace la selección, ¿qué va a decir? ¿Que está mintiendo? Si él no sabe nada...". Ni uno ni otro tienen medida para las horas que pasan ante una computadora cuando hackean. "Llega un momento en que te empiezan a doler las manos y los brazos y suponés que debés estar cansado, entonces pensás que tal vez sea mejor irse a dormir. Y de verdad podés dormir veinte horas", asegura Opii.

Sostienen que esa dedicación obstaculiza el desarrollo normal de otros aspectos de sus vidas, como la relación con el sexo opuesto. No son muchas las féminas que han incursionado en el mundo de los hackers. "Que yo conozca -revisa Janx- hay muy pocas. Argentinas, ninguna. De afuera conozco tres o cuatro, no más. Lo que me hace pensar en lo que decían en el MIT: la proporción de estudiantes mujeres era del 20 por ciento en el primer año y en el segundo bajaba al 10 por ciento."

- ¿Hablan con sus mujeres del hacking?

- Es un aspecto mío que no comparto con las mujeres. Mi última novia sabia algo, que yo hacía una cosa extraña, pero no comprendía qué y yo tampoco le explicaba. Una cosa es hackear y otra cosa es salir... Yo no me considero un enfermo de la máquina: un día salís y otro te sentás adelante de la computadora. Se pueden juntar o no, y en mi caso fue no. No me gustaría salir con una mujer para hablar de temas técnicos, es aburridisimo. Es de lo que estás hablando todo el día. Querés cambiar de tema. No es que no me guste hablar de temas técnicos porque es aburrido: no me gustaría hablar exclusivamente de temas técnicos. Puedo salir con una hacker pero no necesariamente voy a estar hablando de problemas técnicos. No me molestaría compartir la actividad, pero en general las chicas se aburren y se van.

- Cuando salgo con alguien, no tiene nada que ver con hacking, computadoras, teléfonos, ni nada. La persona se va a aburrir y yo voy a perder mi tiempo. Las mujeres te preguntan qué estás haciendo con la máquina; te piden: "Dejá la computadora, ¡veni!". Les resulta aburrido, y tienen razón.

- ¿Tienen razón, es aburrido?

- Es aburrido cuando uno no sabe y el otro sí -aclara Opii.

- Si estoy saliendo con alguien y esa persona no tiene ni idea de este tipo de cosas, no me voy a poner en una máquina a hackear o programar, porque se supone que le tengo cierto aprecio. No voy a hacer que esté aburrida durante tres horas mirándome mientras yo estoy programando... No le voy a decir "Callate que me desconcentrás".

En los años que llevan de hacking conocieron a muchos colegas de otros países, pero se niegan a dar sus nombres. "Hace años -recuerda Opii- había un sistema en Alemania donde entraban hackers de todas partes del mundo, un sistema de charla. Yo entre ahí cuando empecé y conocí a un montón de gente. Después ese lugar dejo de existir, pero hubo otro y después otro, y de repente ya no hubo ninguno mas, por lo menos en cuanto a las redes X.25. Ahora estás por ahí y te encontrás con alguien que recordás haber conocido en otra época. Y te hacés amigos hasta cierto punto. En mi caso, no son amigos de los cuales me fiaría un cien por ciento. De hecho, yo no confío en nadie totalmente." "Los amigos de la computadora -sentencia Janx- son amigos de hacking. De ahí a otra cosa..."

Todo Para el Hacker

En el país, como en el resto del mundo, la comunidad hacker tiene publicaciones que actúan de informadoras y formadoras. Uno de los formatos mas acorde con las actividades que realizan es el electrónico, ya que así pueden recuperar ejemplares de los BBSs que las distribuyen. Es el caso de Minotauro, dirigida por Lapidario y Drako y que se distribuye a través del BBS Dionysios, dedicado principalmente al tema virus pero que mantiene áreas de hacking. Su sysop (el operador del sistema) es Zarathustra, quien en sociedad con Drako instaló otro nodo, Dionysios II, la sede de Minotauro, que se trabaja en formato ASCII. En el editorial del primer número, los directores se presentaban y anunciaban sus intenciones: recopilar información útil y presentarla en un solo lugar. Como no sólo de BBSs y formatos electrónicos vive el hacker, las revistas impresas no están ausentes.

Así como 2600 es la cara de los hackers norteamericanos en papel, en el país la representante es Virus Report, su manual de supervivencia informatica, unica en su estilo. Debutó en 1993 como nuevo producto de MP Ediciones y a partir del numero nueve se independizó para convertirse en una publicación de Ediciones Ubik. Su temática incluye mucho más que noticias sobre y para hackers: también acerca a los lectores material sobre virus informáticos -analizados extensamente-, criticas literarias -ciencia ficción, cyberpunk y novelas basadas en hechos reales de hacking-, comentarios sobre los delitos que se dieron en llamar informáticos y análisis de legislación al respecto. La tirada de cinco mil ejemplares dice que la comunidad argentina de hackers esta aun lejos de alcanzar la importancia de otras en el mundo, pero también demuestra que la vorágine de las comunicaciones telemáticas se acerca a pasos agigantados, aunque el desarrollo tecnológico no sea justamente el del Primer Mundo. Por ser una revista chica (tiene dieciséis paginas), con escaso apoyo publicitario, Virus tuvo en su trayectoria dificultades para llegar al interior del país. Sobre todo los estudiantes de carreras relacionadas con computación -que la transformaron en su texto de cabecera- la esperan todos los meses y no siempre la reciben: mas de una vez el numero no aparece y deben reclamarlo por correo a los editores.

Gracias a las conexiones con Internet, Virus sale del ámbito vernaculo para brindar información sobre lo que pasa en el resto del universo hacker. Reportajes a lideres como Emmanuel Goldstein y notas sobre las reuniones globales organizadas por los holandeses de Hack-Tic suelen poblar sus paginas y son elementales para la actualización y el vínculo de los locales con la realidad global.

En 1993, cuando Virus Report todavía era publicada por MP Ediciones, recibió en su redacción una llamada de alguien que se identificaba como Ivan Hammer. Decía tener un BBS de intercambio de virus, Satanic Brain, y quería que se publicara algo en la revista. En realidad, en ese momento no tenia demasiado: una colección de virus y algunos textos sobre hacking. Su verdadero alias era Azrael y justificaba su BBS como un lugar para aprender. "La idea básica es que la gente que esta interesada en el tema pueda darse cuenta de que la computación no es solamente lo que le dicen -dice Azrael-, no es tener un Windows o un utilitario de ese tipo. Y a los que quieren programar les puede servir para notar que hay lenguajes de bajo nivel que nadie utiliza. En general, el punto es demostrar que se pueden hacer cosas con la computadora, que por medio de un virus se aprende mucho más que programando una base de datos." Satanic Brain y sus operadores se despegaron rápidamente de sus humildes comienzos y crecieron a un ritmo acelerado. La documentación del programa Virus Creation Lab

(VCL, Laboratorio de creación de virus) tenia información sobre cómo contactarse con los BBSs de virus de los Estados Unidos, puente para acceder a NuKE, red de BBSs. Una vez conectados, la relación se fortaleció con diversos intercambios y hoy son coordinadores de NuKE para Latinoamérica. Ser miembro de esa red significaba tener acceso a su base de virus, y ademas, de hacking. "NuKE es un grupo de programadores de virus internacional -explica Azrael-; los trabajos que más se conocen son el Npox, en Estados Unidos, y el VCL de Nowhere Man. Tenemos gente distribuida por todo el mundo: Australia, Europa, Suiza, Africa, los Estados Unidos y Canadá". Los integrantes se mantienen en contacto a través del e-mail, que utilizan una vez por semana. -Tenemos un área de mensajería productiva -cuenta el sysop de Satanic Brain-, donde se tratan cosas que pueden ayudar a la gente que esté interesada en el tema.

- ¿Quién se entera de lo que ustedes hablan por e-mail?

- Cualquiera puede leerlo; una persona que hace antivirus puede acceder y sacar material de virus nuevos que estamos haciendo. Y también hacemos trabajos en común.

Pero NuKE no se dedica exclusivamente a virus: el grupo tiende cada vez mas al hacking. Y Satanic Brain no podía ser menos. En la actualidad, cuenta con la gente de HBO como sysops en el área de hacking, en especial Opii. El BBS cambia permanentemente. Azrael instala software nuevo cada semana, con lo que obliga a los viejos usuarios a volver a registrarse. El efecto es que los únicos que permanecen son los conocidos y amigos de Azrael. A pesar de sostener que la información sobre virus debe regalarse y ponerse a disposición de todos, mantiene un constante ataque a los "lamers", usuarios nuevos que no saben mucho del tema. Es extremadamente difícil acceder a la información del BBS, y mucho mas si el que la busca no demuestra tener los conocimientos que conforman a su operador.

La gente de Minotauro y Dionysios formó un grupo de hacking y virus llamado DAN (Digital Anarchy, Anarquía Digital), que en cierta medida pretende competir con Nuke en el nivel nacional. Su fuerte es la creación de virus, pero tienen un gran interés en el hacking. Por el momento, las actividades que organizan son escaneos de números 800 (gratuitos, recientemente instalados en el país) e intentos de hacking a tarjetas telefónicas.

El Primer Encuentro

En octubre de 1994, Virus Report se coloco a la cabeza del movimiento al organizar el Primer Congreso sobre Hacking, Virus y Computer Undeground del país, que se desarrolló en el Centro Cultural Recoleta de Capital Federal. Durante tres días, los habitués del Centro se vieron sorprendidos por muchachos de pelos muy largos y remeras estrafalarias que ganaron los pasillos en grupos y nunca abandonaron sus teléfonos celulares. El microcine del Centro, con capacidad para ciento cincuenta personas, fue desbordado desde el primer dia. Con anuncios en casi todas las radios y diarios, el congreso convocó a un promedio de trescientos asistentes por jornada, casi la mitad de ellos provenientes de las provincias con ansias de recoger información para sus estudios o, en el caso de los profesores, para las escuelas donde desarrollan su actividad.

La intención de los organizadores era lograr un encuentro internacional, nada fácil si se tiene en cuenta la enorme distancia entre este país y los desarrollados, hecho complicado por la ausencia de fondos para solventar pasajes y gastos de los invitados extranjeros. Sin embargo, hubo importantes visitas: el

famoso Emmanuel Goldstein, Mark Ludwig -especialista en virus informáticos y autor de libros sobre el tema- y Patrice Riemens, uno de los organizadores del Galactic Hacker Party de 1989. Ellos pagaron sus viajes y aquí recibieron alojamiento en los voluntariosos hogares de amigos y colegas. El congreso abrió sus sesiones con un tema candente en los Estados Unidos: encriptación de datos y el programa PGP. Daniel Sentinelli -asesor de seguridad informatica- y Leandro Caniglia -programador y doctor en matemáticas- explicaron los principios básicos del PGP y dieron una visión matemática para aclarar en que se basa la cuestión de claves publicas y privadas. En momentos en que la comunidad informatizada de los Estados Unidos debate el derecho del gobierno para imponer una encriptación exclusiva, cuyas claves quedarían en poder de los servicios de información norteamericanos, la charla constituyó una excelente oportunidad para entender la cuestión y clarificarla. Mark Ludwig se explayo, poco después, en un análisis sobre los virus informáticos y su relación con la vida artificial, tema central de su segundo libro Computer Virus, Artificial Life and Evolution. Aquellos que esperaban una explicación rápida y sencilla de como crear virus, quedaron un tanto decepcionados. Ludwig fue un expositor de alto nivel académico. La mesa sobre revistas del underground computacional generó una discución de principios: ¿es licito cobrar los ejemplares cuando se está a favor de la libre información? Las opiniones de Lapidario y Drako, en representación de Minotauro, Martín Salías y Fernando Bonsembiante, por Virus Report, y Mark Ludwig, por Computer Virus Development, no alcanzaron para clarificar el tema y la contradicción quedo sin resolver. Lapidario, para reforzar su postura a favor de la gratuidad, regaló diskettes con el ultimo numero de Minotauro y sostuvo que el objetivo era que la gente con escasos conocimientos pudiera aprender rápido sin tener que llamar permanentemente al BBS para plantear sus dudas. Pero hubo otros momentos de mayor emoción y que ganaron la atención de todo el mundo.

- Ahora que nadie nos escucha podemos hablar sobre el lavado de ese dinero.

- Bueno, que te parece si…

Las voces se difundían a través de los parlantes del microcine y la conversación por teléfono celular entre Daniel Sentinelli y Fernando Bonsembiante se interrumpió por las carcajadas de los presentes. La demostración que hizo Pablo Untroib -radioaficionado- en la charla sobre telefonía celular y phreaking dejó en claro que no hay tecnología que se resista al ingenio y audacia de los que no dejan de investigar. Pablo colocó su aparato en modo test, lo que permite hacer con el teléfono cosas que normalmente están reservadas a los técnicos. Con este truco pudo captar la comunicación entre los otros dos, alejados de la mesa. Goldstein reforzó los ejemplos interceptando durante segundos varias conversaciones anónimas. El mito de la seguridad en la telefonía celular se había roto.

La mesa sobre hackers, con Goldstein y Riemens como participantes excluyentes, fue la que concitó mayor atención y se prolongo mas allá de lo esperado. El líder norteamericano calificó la situación de su país como "densa". En este momento, reseño, "hay algunos hackers presos por el miedo y el desconocimiento de quienes legislan y gobiernan. El miedo de todo tipo de gobierno es que la gente pueda tener información". Al respecto señaló que pocos meses antes había visitado el Congreso norteamericano para alertar a los legisladores sobre la inseguridad de los teléfonos celulares pero, en lugar de escucharlo, lo reprendieron por publicar supuestos códigos secretos en su revista. "La mayoría de los hackers somos egoístas, pero no malos. Eso es lo que no puede entender el gobierno de Estados Unidos", dijo Emmanuel y recordó a su amigo Phiber Optic, quien en ese momento cumplía una

condena de un año de prisión. Se ocupó de dar la dirección a la cual escribir a Phiber y pidió que lo hicieran porque "la felicidad de los presos al recibir una carta es infinita".

- ¿Cómo sabes? ¿Estuviste preso? -le preguntaron.

- No por hacker -contestó Goldstein-: por participar de una protesta contra la instalación de una planta nuclear. Salí enseguida, pero pude observar lo que sucedía con el correo allí dentro.

Patrice Riemens -quien negó ser un pionero del hacking holandés y dijo estar cerca del movimiento por sus características de contestatario y antisemita- destacó la actividad del grupo Hack-Tic como un buen ejemplo para cambiar la imagen que la sociedad tiene de los hackers. Los holandeses crearon una fundación, adquirieron los derechos para constituirse en proveedores de acceso a Internet a precios económicos y llegaron a convertirse en el principal representante de esa red en Holanda.

Pero no todo fueron rosas en el congreso. Algunos de los integrantes mas jóvenes de la comunidad que durante los meses de organización se habían opuesto a que se realizara el encuentro protagonizaron algunos intentos de boicot. El primer día y a poco de comenzar, un socio de Azrael accionó un matafuegos, supuestamente sin quererlo, cuando un amigo brasileño estaba por sacarles fotos. No sólo llenó de polvo blanco a los que estaban alrededor sino que casi los ahogó, además de generar malestar y protestas en los responsables del Centro Cultural, quienes amenazaron veladamente con suspender el encuentro. No lo hicieron y, ante la continuación del programa, los chicos siguieron pensando como podían señalar su presencia. El último día dieron una sorpresa.

- En el teléfono público del hall central hay un mensaje para este congreso -le dijeron a Bonsembiante en un entreacto.

Al levantar el tubo había que aguardar el "espere un momento" y entonces apretar el botón de volumen. El visor, cuadro a cuadro, permitía leer:

```
"The quick browm fox jumps over the lazy. dog. (El zorro
marron rapido
salta sobre el perezoso. perro.) Esta conferencia sucks
(huele feo), como
todas las conferencias de 'hackers'. Y eso no tiene nada que
ver con las
buenas intenciones de F.Bonsenbiante: es simplemente que
hablar acerca de
los hackers es pointless (insustancial). Los hackers no somos
ni queremos
ser rock stars y toda esa publicidad barata se la pueden
meter en el culo,
    no la necesitamos ni nos hace bien. Es logico que los que
no saben
    quieran saber que es un hacker. Bueno, vamos a
intententar una definicion:
    toda persona curiosa es un hacker potencial. La
```

tecnologia nos la venden
con etiquetas que nos dicen para que usarla: todo eso es mentira. La
tecnologia es solo una herramienta y hay que saber darla vuelta y usarla
del otro lado. Todos escucharon que la información debe ser libre: eso
solo significa que todos tenemos que poder elegir el pasto del que
comemos. La investigacion en ciencias es una de las actividades
intelectuales mas gratificante y todos los investigadores son en cierta
medida hackers. Si el gobierno anuncia ahora que privatiza la CNEA porque
lo mando el Banco Mundial, si Cavallo manda al CONICET a lavar los platos,
y todo eso es tan legal, nos preguntamos quien es quien para juzgar la
legalidad de un grupo que lo unico que busca es el conocimiento. Desafiar
las leyes en las que uno no cree es la unica manera de seguir creyendo en
uno mismo y no convertirse en un pedazo de sillon, para que venga alguien y se siente arriba.

Manifiesto HBO. Hacked by Owls.

Sres. de Telecom:
Esperamos no tomen a mal nuestro atrevimiento. Nuestra intencion no era
causar inconvenientes, si no dar a conocer nuestro mensaje de una manera
acorde a la forma de pensar de la gente a la que queriamos llegar. Para
minimizar los inconvenientes elegimos un teléfono fuera de servicio".

- Si la idea era dejar un mensaje ¿por qué hacerlo tan complicado? -le preguntaron a Opii.

- ¿Qué mensaje? ¿Porque me preguntas a mí?

- Porque lo firma HBO.

- ¿Y yo qué tengo que ver con HBO? -respondió, en un intento de separarse de la situación. Pero de inmediato dio una opinión que, aclaró, era su punto de vista sobre un hecho en el cual no estaba involucrado: "Supongo que la cuestión era que lo leyera la gente a la que iba dirigido", dijo.

- Si no anunciaban en público la forma de lograrlo, hubiera sido imposible...

- Pero se anunció, y el que lo quería leer solo tenía que averiguar cómo.

- ¿No estas de acuerdo con la realización del congreso?

- En principio no, porque me parece que estas cosas logran llamar la atención y eso no nos beneficia.

- ¿Te pareció malo?

- No, estuvo bastante bien, pero yo lo hubiera hecho de otra forma. Acá hubo mucho bla bla y poca demostración. Me parece que para hacer algo así hay que organizarlo de otra manera... Qué se yo, alquilar un galpón grande, instalar varias máquinas en red, tener acceso a Internet... algo parecido a un workshop. Si no, no tiene sentido.

Si es Viernes es Virus

Los hackers locales siguen los pasos del movimiento mundial, en ocasiones tal vez demasiado puntillosamente: así como los lectores de 2600 se reúnen los primeros viernes de cada mes en algún lugar público para intercambiar experiencias, en Buenos Aires comenzaron a organizarse durante 1994 reuniones de lectores de Virus Report. En principio se anunciaron como encuentros de seguidores de 2600, pero luego se transformaron en mitines de lectores de las dos revistas. Allí se juntan Azrael, Opii, Zarathustra, Drako, El Chacal, asesores en seguridad que trabajan para grandes empresas y todo tipo de gente. La cita es a partir de las 17 horas en un bar cerca del Congreso. Quizá sea el único momento en el que es posible ver a integrantes de PUA, HBO, NuKE y DAN en una misma mesa. Lo que no significa que haya paz. El Chacal siempre discute con los HBO, Azrael critica a los DAN, estos se quejan del elitismo de Azrael. Pero el clima general es bastante tranquilo. Se intercambian diskettes, CD-ROMs, cintas de backup; sacan fotocopias a montones (para el beneplácito de la fotocopiadora vecina al bar) y, sobre todo, charlan hasta por los codos. Siempre hay un grupito hablando de virus y otro de hacking. Nunca falta el alarmista que anuncia "una razzia de la policía en cualquier momento". Pero la Argentina no es los Estados Unidos y la falta de leyes sobre el hacking protege a los asistentes. De todas maneras, nadie hace hacking en la reunión ni toca alguno de los dos teléfonos públicos del bar y casi nunca hay computadoras. Es el lugar ideal para hablar de presentes y futuros. En estos dias El Chacal es un reconocido asesor de seguridad informática para empresas y afirma que el costo por el uso de líneas telefónicas y de tiempo de computadora es algo contemplado por cualquier empresa. Del hacking rescata la manera de estructurar los conocimientos y reconoce que su actual posición económica se debe indirectamente a sus tiempos de hacker; asi pudo adquirir conocimientos que hoy aplica a otros ámbitos, como el desarrollo de técnicas de seguridad. "Técnicas de seguridad infalibles", se burla para aclarar de inmediato que no existe nada absolutamente seguro. Se manifiesta, todavía, a favor del libre flujo de la información, aunque reconoce que hace pocos años era un poco mas anarquista y romántico.

- Hackear tiene algo de voyeurismo, una gran cuota de satisfacción intelectual. Es una necesidad básica, como el sexo, la comida, la droga y el rock & roll -compara.

- ¿Porqué sos asesor entonces?

- Con el tiempo un hacker se aburre de mover solo sus piezas, sin tener respuesta. Por eso se transforma en asesor de empresas: para hacer la jugada de ataque y también tener el desafío de diseñar la defensa. Es como jugar al ajedrez: si ganas dándole con las piezas por la cabeza al otro no tiene gracia. El hacking es un desafío intelectual.

Sticky confiesa que ya abandono la actividad porque "cuando tenés pibes no podes estar haciendo un chat (conversación por módem), concentrado, sin fijarte si alguno de ellos se te rompe la cabeza. Además yo no era un hacker, me interesaba copiar programas y mirar lo que hacían los otros, nada mas". Ni nada menos. Truchex se dedica a programar sistemas comerciales y administrativos y tiene un BBS al que le dedica sus ratos libres los fines de semana. Afirma que no volvió a tener contacto con los hackers extranjeros y cree que eso le paso a todos una vez que superaron los veinte años. "Yo me río mucho cuando oigo hablar de los nuevos hackers -dice-. Los veo tan ridículos y gansos. Me río cuando me doy cuenta que están haciendo exactamente las mismas cosas, que maravilloso. Yo no podía entender que a otra gente le pareciera mal. Me parece que los años no vienen solos, estoy hecho un viejo de mierda."

VI. Hackear (Y) la Ley

"Si seguimos haciendo que el acceso a la tecnología sea difícil, burocrático e ilógico, habrá mas crímen informático. Por la sencilla razón de que si se trata a alguien como un criminal comenzará a actuar como uno. Si convencemos a la gente de que copiar un archivo es lo mismo que robar, físicamente, algo, no podemos sorprendernos cuando una definición tan amplia redunda en mas crimen en sentido amplio. Desdibujar el limite entre una infracción virtual y un crimen verdadero es un error."

CARTA DE EMMANUEL GOLDSTEIN
AL CONGRESO DE LOS ESTADOS UNIDOS

"Todas las áreas dependen hoy, sabiamente o no, de sistemas informáticos. El dinero, las carreras y posiblemente inclusive sus vidas dependen del funcionamiento permanente de las computadoras. Como sociedad, no podemos darnos el lujo de perdonar o estimular conductas que amenacen o dañen los sistemas informáticos. Como profesionales, los científicos y los ingenieros de computadoras no podemos darnos el lujo de tolerar que se haga una figura romántica de los vándalos y criminales de las computadoras."

EUGENE H. SPAFFORD EN
THE INTERNET WORM PROGRAM: AN ANALYSIS
(EL PROGRAMA DEL GUSANO DE INTERNET: UN ANALISIS)

Estados Unidos

Mas de un trillón de dólares se mueve por semana alrededor del mundo electrónicamente. En los Estados Unidos cada año se pierden cuatro mil millones de dólares en datos robados y soft pirateado. Paul Saffo, investigador del Instituto para el Futuro de Menlo Park, California, sostiene que "nadie tiene idea de lo que se puede hacer con un sistema hasta que una banda de chicos empieza a jugar y a descubrir formas de ingresar. Ese es el ciclo: primero los exploradores, despues los ladrones, y, por

ultimo, la policía". De acuerdo con Donn Parker, promotor de Gail Thackeray -ayudante de la fiscalía durante el operativo Sundevil y experta en seguridad computacional- el primer abuso de una computadora se registró en 1958 mientras que recién en 1966 se llevó adelante el primer proceso por la alteración de datos de un banco en Mineápolis. En la primera mitad de la década del 70, mientras los especialistas y criminólogos discutían si el delito informático era el resultado de una nueva tecnología o un tema específico, las intrusiones computacionales se hicieron mas frecuentes. Para acelerar las comunicaciones, enlazar compañías, centros de investigación y transferir datos, las redes debían -y deben- ser accesibles; por eso el Pentágono, la OTAN, las universidades, la NASA, los laboratorios industriales y militares se convirtieron en blanco de los hackers. Pero en 1976 dos hechos marcaron un punto de inflexión en el tratamiento policial de los casos: el FBI dictó un curso de entrenamiento para sus agentes acerca de delitos informáticos y el senador Abraham Ribicoff -junto con el Comité de Asuntos del Gobierno de la Cámara- presentó dos informes que dieron lugar a la Federal Systems Protection Act Bill (Ley Federal de Protección de Sistemas) de 1985, base para que Florida, Míchigan, Colorado, Rhode Island y Arizona se constituyeran en los primeros estados con legislación específica; anticipándose un año al dictado de la Computer Fraud y Abuse Act de 1986.

El acta se refiere en su mayor parte a delitos de abuso o fraude contra casas financieras o involucradas en delitos interestatales. También específica penas para el tráfico de claves con intención de cometer fraude y declara ilegal el uso de passwords ajenas o propias en forma inadecuada. Pero sólo es aplicable en casos en los que se verifiquen daños cuyo valor supere el mínimo de mil dólares. El aumento en la cantidad de casos de hacking y la sensación de inseguridad permanente que generaron -fomentada por la difusión de los hechos en programas especiales de televisión y artículos de revistas especializadas-, cambiaron la percepción de las autoridades con respecto a los hackers y sus intrusiones. Uno de los casos que demostró ese cambio, con escasa publicidad, fue el de Kevin Mitnick. La primera vez que lo detuvieron fue en 1981 por robar manuales de la Pacific Telephone y tuvo que cumplir seis meses de prisión; en 1983 intentó ingresar en las computadoras de la universidad de California del Sur y poco después penetró el sistema de la agencia de créditos TRW; en 1987 lo condenaron a treinta y seis meses de libertad condicional por robo de soft; hackeo los sistemas de la North American Air Defense (NORAD, Defensa Aerea Norteamericana), el Departamento de Defensa y la NASA.

La justicia libró una orden de captura en su contra, acusándolo de usar su magia tecnológica como arma y de violar los términos de su prueba federal. Lo arrestaron en 1988 y un año después lo condenaron a dos de prisión. Durante ese tiempo le negaron el acceso a los teléfonos y a lo largo de los doce meses de rehabilitación no pudo acercarse a una computadora. La dureza en el trato hacia Kevin Mitnick contrasta con aquella condena a Captain Zap de libertad vigilada por teléfono, y preocupó a la comunidad hacker, que consideró la avanzada legal como una forma más de caza de brujas. Pero el primer caso en que se puso a prueba el Acta de 1986 fue el de ShadowHawk (Herbert Zinn Jr.). Después de dos meses de control policial, pinchadura de teléfono y monitoreo de su computadora, se lo acusó de ingresar ilegalmente en Bell Laboratories, AT&T y las compañías telefónicas de Illinois y Rochester, con el agravante de copiar documentos considerados "sensibles". Durante el juicio, en 1989, valuaron esa información en un millón de dólares y, a pesar de que ShadowHawk no lo había vendido, se concluyó que había existido "intento de fraude" y fue condenado a nueve meses de prisión y una multa de diez mil dólares.

Confiados en este antecedente, los investigadores de Sundevil llevaron al estrado el caso de Craig Neidorf. Cuando The Prophet le paso a Knight Lighting un documento de la compañía telefónica, ambos fueron acusados de acuerdo con el artículo 18 de la sección 1029 del Acta, pero allí se especifican dos limitaciones: el delito debe afectar dentro del estado o al comercio exterior (el robo de líneas de larga distancia afecta el comercio interestatal de la Telco), y la pérdida o daño debe tener un valor mínimo de mil dólares, por eso la acusación valoró el documento E911 en setenta y nueve mil. El artículo establece, además, que no es ilegal usar aparatos para realizar fraudes, pero si construirlos. "Producir, diseñar, duplicar o armar" blue boxes son crímenes federales hoy en día. La sección 1030, "Fraude y actividades relacionadas con las computadoras", le dió jurisdicción directa a los servicios secretos sobre los casos de intrusión computacional. Fue el camino elegido por el Senado para liberarse del problema: dejaron que los servicios secretos y el FBI se pelearan entre ellos; el resultado fue que el FBI mantuvo jurisdicción exclusiva cuando el delito se relaciona con la seguridad nacional, espionaje extranjero, bancos federales asegurados y bases militares. El artículo establece que es ilegal el "Acceso a una computadora sin autorizacion" si es de una institución financiera o de una compañía de tarjetas de crédito (fraudes).

De acuerdo con el criterio de los analistas legales, la diferencia con las "de interés general" (gobierno, redes interestatales) se marcó porque al Congreso no le interesa que los servicios secretos investigaran sobre todas las intrusiones. El FCIC (Federal Computers Investigation Comitee), una organización poco ortodoxa y nada burocrática, es la más importante e influyente en lo referente a delitos computacionales: los investigadores estatales y locales, los agentes federales, abogados, auditores financieros, programadores de seguridad y policías de la calle trabajan allí comunitariamente, sin categorías que estorben. Sus integrantes -que muchas veces se hacen cargo de los gastos para dar conferencias en otros estados- están convencidos de que gracias a ese funcionamiento pueden hacer su trabajo. El FCIC no acepta subvenciones y nadie sabe el número exacto de miembros; no tiene jefe, presupuesto ni horario, sólo una casilla de correo en Washington en la División de Fraudes del Servicio Secreto. Pero es la entrenadora del resto de las fuerzas policiales en cuanto a delitos informáticos, y el primer organismo establecido en el nivel nacional. Se mueve con tres grupos básicos: entrenadores, agentes de seguridad e investigadores. Enseñan al resto de las organizaciones y fuerzas policiales cómo trabajar en el ámbito informático, con indicaciones importantes para la policía callejera, que en mas de una ocasión encuentra computadoras en sus operativos. Para los secuestros de equipos recomiendan cuidar la evidencia, fotografiar todo, ponerle nombres a todos los cables, no dejar diskettes en campos magnéticos ni escribir sobre ellos con biromes; secuestrar manuales, impresiones y notas manuscritas; copiar la información y trabajar sobre el duplicado, guardando los originales.

Los agentes del FCIC utilizan los mismos métodos que los hackers: pinchaduras de líneas telefónicas y fibras ópticas, monitoreo de computadoras y BBSs, trashing y hasta ingeniería social. Siempre tienen en cuenta -y buscan hasta hallarlo- el informante interno (en casos de BBSs) que les brindara los datos necesarios. Bruce Sterling tuvo oportunidad -mientras investigaba para su libro The Hacker Crackdown- de asistir a una conferencia del FCIC, en la que uno de los agentes demostró como se pinchan las fibras ópticas. El hombre distribuyó un cilindro metálico de un dedo de largo con dos tapas en las puntas (de una de las cuales salían tres cables negros tapados con un pequeño plástico negro), parecido a un multiplexor (aparato para duplicar señales). Se hace un corte en la fibra y se conectan dos

de los cables negros para continuar la red; el tercero, explicó, va a un monitor que permite ver toda la información que pasa.

La experiencia de los investigadores marca que las tapas de acceso a los tendidos de cables subterráneos son especialmente vulnerables en los Estados Unidos. Hace pocos meses una empresa telefónica de Nueva York descubrió que una compañía de cables usaba su red para brindar el servicio sin pagar royalties. Una compañía de seguridad de New England diseño el "intimidador", un tornillo de acero cuya cabeza admite solo una herramienta especial, identificada con un numero y guardada por el fabricante.

Muchas otras organizaciones trabajan en el territorio de los Estados Unidos Unidos, aunque en áreas mas especificas. La Asociación Internacional de Especialistas en Investigación Computacional (IACIS) investiga nuevas técnicas para dividir un sistema en sus partes sin destruir las evidencias; sus integrantes son una especie de forenses de las computadoras y trabajan, además de los Estados Unidos, en el Canadá, Taiwán e Irlanda. La Oficina de Investigaciones Especiales (OSI) es la única entidad federal dedicada full-time a la seguridad computacional. DATTA, una asociación de abogados de distrito, se especializa en robos de chips, propiedad intelectual y mercado negro. En Silicon Valley opera la Asociación de Investigadores de Computadoras de Alta Tecnología (HTCIA); en Florida, Illinois, Maryland, Texas, Ohio, Colorado y Pennsylvania se mueve el Law Enforcement Electronic Technology Assistance Comitee (LEETAC, Comité de Asistencia para el Cumplimiento de la Ley en Tecnología Electrónica). Las leyes norteamericanas contemplan casi todas las áreas donde pueden darse delitos informáticos: jurisdicción marítima; bancos; propiedades o registros federales; la adquisición de falsa identidad de empleado estatal u oficial; el uso de cables que crucen líneas estatales para cometer fraude o robo bajo falsas pretensiones; el daño malicioso a propiedad federal; el ocultamiento, la mutilación, la copia o el cambio de lugar de registros públicos. Uno de los temas que mas preocupan -tanto en el ámbito legal como en el comercial- sigue siendo el uso indebido de líneas telefónicas.

Henry Kluepfel, de Bell Comercial Research, estima que el robo de llamadas de larga distancia cuesta a empresas y clientes más de quinientos mil millones de dólares anuales; los servicios secretos dicen que son dos mil millones y las industrias amplían la cifra a nueve millones. En 1984 los bancos y empresas norteamericanas gastaron seiscientos millones en sistemas de seguridad y se calcula que en 1993 invirtieron mas de dos mil millones. El área metropolitana de Nueva York, vanguardia del crimen informático norteamericano, dice ser objeto de ciento cincuenta mil ataques físicos a teléfonos pagos por año. La preocupación por el tema es de tal magnitud que ya proliferan en empresas y bancos los auditores de sistemas telefónicos que regulan sus honorarios en un porcentaje sobre el ahorro que esas compañías logran a través de sus servicios. Ya no hay una clara división entre phreakers y hackers, asi como no es clara la separación de teléfonos y computadoras: estas aprendieron a hablar a través de las lineas. Segun Jenkins, del servicio secreto, hay algo peor: algunos hackers aprendieron a robar y algunos ladrones a hackear. Los manuales de entrenamiento de los agentes federales presentan a los BBSs como centros operativos de delitos, pero no todos los agentes coinciden. Muchos consideran que el secuestro de los Bulletin Board atenta contra la libertad de expresión. Los operativos como Sundevil crearon serios problemas de relaciones publicas a los servicios, ya que los usuarios los consideraron un atropello y violación a la privacidad porque junto al BBS se secuestró el correo electrónico.

En general, los procedimientos antihacker siguen una guía. Primero, el personal policial ingresa casi con violencia y por todas las puertas de la casa que se va a requisar; el argumento es que de esta manera son mínimas las chances de desgracias. Luego la prioridad es alejar a los sospechosos de las computadoras para que no destruyan evidencias: Un guardia -que les lee sus derechos- se los lleva a algún lugar de la casa donde no haya máquinas. Dos oficiales se ocupan de los equipos y sus periféricos, conectados o no a lineas telefónicas. Uno de ellos es, casi siempre, el que gestionó la orden judicial, y por tanto sabe que tiene que buscar; el otro fotografía los aparatos y el resto de la casa para evitar reclamos posteriores.

Estos policías, tan acostumbrados a obedecer reglas y órdenes, con el autoritarismo grabado como método de relación, se encuentran con serios problemas y contradicciones cuando ingresan en el mundo de la telemática: allí no hay reglas fijas ni leyes establecidas; mal que les pese, son tan pioneros como los hackers. En su libro Bruce Sterling cuenta una anécdota: uno de los agentes del FCIC le comento que "en el mundo de la policía todo es blanco y negro, bueno y malo. En el mundo de las computadoras todo es gris." Tal es así, que aun cuando logran encarcelar a algún hacker, no están a salvo de sus intrusiones. Scott Robinson accedió a la terminal de la cárcel de Santa Clara mientras cumplía su condena y modificó la fecha de finalización de su prisión del 31 al 5 de diciembre. Arrestado nuevamente, dijo en su descargo que quería pasar Navidad con su familia. Emmanuel Goldstein asegura que desde 1983 no quebró la ley y que no es necesario hacerlo para ser un hacker.

- En los Estados Unidos se vuelve cada vez mas difícil, porque todos los días aparecen mas leyes restrictivas. Por ejemplo, escuchar ciertas frecuencias es ilegal; son leyes estúpidas y deben ser violadas -asegura.

- ¿Por qué?

- Porque no tienen sentido, fueron escritas y votadas por gente que no entiende a la tecnología. Captar las frecuencias de teléfonos celulares es ilegal pero no hay forma de cumplir con esa ley ni de aplicarla, porque con sólo prender la radio estás registrando una o varias frecuencias. La respuesta correcta es encriptar las comunicaciones para que no puedan ser escuchadas. Cuando fui al Congreso para alertar sobre la posibilidad de que se intercepten conversaciones, los legisladores, en lugar de escucharme me insistían: "Emmanuel, ¿por que violas las leyes publicando códigos que son secretos?". Les contesté que todo lo que yo había publicado aparecía en los manuales y otros libros, que nada de eso era secreto, y al fin se aburrieron: "Bueno, está bien". Obviamente no entendieron de que se trataba.

- ¿Qué tipo de leyes hacen falta?

- Leyes que reflejen lo que ya existe, que no agreguen penas por el solo hecho de usar una computadora, que es nada mas que una herramienta. El estafador va a estafar con o sin computadora.

De acuerdo con las especificaciones de las leyes norteamericanas, las figuras penales en las que puede encuadrarse el accionar de un hacker son:

- **Daño criminal o malicioso**. Se refiere a la destrucción intencional de la propiedad de otra persona. Deben constatarse tres cosas: acción humana real, evidencia del daño y que este sea observado por un tercero.

- **Robo**. A menos que haya una clara intención delictiva por parte del hacker, es muy difícil lograr una condena con esta acusación. El debate se centra en si las redes se consideran propiedad privada; muchos interpretan que usar una identificación o password ajena es lo mismo que abrir la puerta de una casa. ¿Es sinónimo de robo? Todavía no está resuelto (el debate de once días a través de WELL trató sobre este tema).
- **Fraude**. Se define así a cualquier tipo de engaño o comportamiento desleal con intención de dañar a otro. Aquí se encuadran la ingeniería social -si la información obtenida se usa para acceder a una computadora y se puede probar algún daño- y el uso de una clave ajena (Fry Guy fué acusado de fraude).
- Hurto. Para calificarlo de esta manera, el hecho debe reunir dos condiciones: la sustracción de alguna propiedad y la intención de privar a su dueño de ella. En las actividades de los hackers se aplica a las modificaciones en los programas para, por ejemplo, generar una copia de la password y luego acceder a ella, o al tiempo de uso de una computadora, servicio telefónico o energía eléctrica.
- **Robo de secretos comerciales**. Se puede incluir en hurto si los secretos se consideran propiedad privada y en ese caso, alcanzan tanto a la sustracción física como a la copia no autorizada.
- **Recibo de propiedad robada**. El receptor debe saber, o sospechar razonablemente, que la propiedad es robada y aceptarla con la intención de privar al dueño legítimo de su tenencia. También puede incluirse en hurto, pero las especificaciones resultan casi ideales para acusar a cualquier hacker, ya que se puede aplicar a todo tipo de propiedad, sean secretos comerciales, información, mercaderías, servicios, tiempo de computadora, claves, archivos, tarjetas o información de créditos (fue uno de los cargos contra Craig Neidorf).
- **Robo de servicios o trabajo con falsos pretextos**. Es una forma de hurto. Puede ocurrir cuando un hacker muestra una falsa credencial para acceder físicamente a una computadora en, por ejemplo, una universidad.
- **Interferencia con los estatutos de uso**. Cuando una persona no puede usar su propiedad porque otro hizo algo que se lo impide, se interpreta que hay una interferencia. Cambios o anulaciones de claves para que alguien no pueda acceder a una red o computadora. Se aplica aún sin daño visible.
- **Conspiración**. Se entiende cuando dos o mas personas combinan o planean un acto fuera de la ley. Los usuarios de un BBS que discuta sobre el hacking pueden ser encuadrados en esa figura (fue una de las acusaciones contra los integrantes de la League of Doom).

Gran Bretaña

Mientras en los Estados Unidos se planificaba el operativo Sundevil, Mad Hacker -confiado por la resolución del juicio contra Steve Gold y Triludan- enloquecía a los responsables de sistemas de ochenta universidades, centros de investigación y escuelas técnicas de Gran Bretaña interconectados por medio del Joint Academic Network (JANET, Red Academica Conjunta). Su debilidad eran las ICL 3980, las mayores mainframes del momento, y solo hackeaba ese tipo de máquinas, ignorando a los demás que cruzaba en su camino. Mad no era un hombre adinerado ni bien equipado: tenia nada mas que una Commodore Amiga 1000 conectada a un módem, pero contaba con ingenio suficiente como

para usarla de base de lanzamiento en sus viajes. El puente para llegar hasta JANET fue un colegio cercano a su casa, el Queen Mary College (QMC) en el que ingreso a través de una cuenta default que, después de unas horas, le permitió obtener privilegios de manager system. Allí genero cuatro usuarios a nombre de Alan Dolby para saltar con ellos a la red y llegar hasta las ICL de las universidades de Glasgow, Nottingham, Belfast y Bath, entre otras.

"El objetivo es tratar de conseguir la categoría máxima dentro del sistema -decía Mad Hacker-, la de director; una vez que la obtenés, no seguís las reglas sino que las dictás, es un juego con el sysman." Bob Jones era el jefe de programadores del QMC y tenía por entonces treinta y ocho años, su etapa de jugar había pasado. Cuando descubrió cuatro archivos AD no tardo en averiguar que eran los usuarios que Mad había creado para acceder a JANET; informó a Jeremy Brandy -director de informática del colegio- y entre ambos optaron por controlar las expediciones del hacker sin cerrarle el ingreso, aunque le quitaron la categoría de mánager. También decidieron grabar las intrusiones y borrar tres de las cuentas. El jefe de seguridad del QMC, por su parte, informo a la Computer Crime Unit (CCU, Unidad de Delitos en Computadoras) de Scotland Yard. Esa dependencia se había creado en 1971 pero en ese momento contaba con sólo cuatro agentes, entre ellos John Austen, a quien se designo para seguir el caso. Austen involucró a la British Telecom, porque la mejor manera de pescar al intruso era controlando las líneas telefónicas. Mad Hacker se dio cuenta de que lo habían descubierto pero, lejos de amedrentarse, ganó confianza en sí mismo. Su atrevimiento fue en aumento. "Creo que deberían saber que estoy loco, y también deprimido" fue la frase que se repetía por centenares en los papeles de la impresora conectada a la computadora del QMC cuando Bob Jones ingresó en la oficina una mañana. "Acepto el reto. Esto les llenará su asqueroso sistema", leyó el responsable del área en la Universidad de Hull al revisar su correo electrónico: Mad había cargado en la máquina un rabbit (conejo), programa que provoca procesos inútiles y se reproduce -como los conejos- hasta que agota la capacidad de la máquina. Quiso hacer lo mismo en el server de la Universidad de Glasgow, pero el operador de turno anuló su intento. Noches después Roger MacKenzie -el director del sistema de Glasgow- trató de ingresar desde su casa y tecleó la contraseña. "Lockout" le respondió la pantalla: Mad Hacker había anulado su cuenta.

El correo electrónico de Bob Jones, mientras tanto, se llenaba con mensajes: "Que E.T. llame a casa", "Que Norman Bates se presente en las duchas", "¿Por qué no me sacan?", eran los mas comunes. Pero Jones no quería anular la entrada, quería pescarlo. El mismo objetivo tenía Austen; algunos de los mensajes de Mad daban a entender que había penetrado en las computadoras del Ministerio de Defensa y el MI5, uno de los servicios de inteligencia británicos, y los de Scotland Yard no estaban dispuestos a permitir que continuara. El 6 de julio de 1988 a las ocho de la noche, el padre de Nick Whiteley estaba sentado en su sillón favorito mirando televisión mientras su esposa cocinaba y su hijo permanecía -como casi siempre a esa hora- en su habitación. Los golpes en la puerta sobresaltaron a todos. ¿Por qué tan insistentes? ¿Por qué no tocaban el timbre?

- Buenas noches. ¿El señor Whitelet? -lanzó, sin mas preámbulos, un hombre vestido con elegante traje.

- Así es. ¿Puedo saber quién pregunta? -contestó el padre de Nick en shorts y zapatillas.

- Agente de Scotland Yard. Tengo una orden judicial para arrestar a Nicholas Whiteley. Cuando Nick leyo el papel largó la carcajada.

- ¿"Daños criminales"? Esto no es para mí, acá debe haber una confusión- razono en voz alta el muchacho.

Tenía diecinueve años y su único pecado había sido jugar con las ICL 3980 de la red JANET, pensó. Pero el monto estimado de los daños alcanzaba a sesenta mil libras, algo más de cien mil dólares. Después del arresto y secuestro de equipos, Nick quedó en libertad bajo fianza, pero en 1990 fue juzgado y condenado a un año de prisión con ocho meses de libertad condicional. Paso dos meses en las cárceles de Brixton y Wandsworth, donde sufrió presiones por parte de otros internos para que difundiera sus conocimientos, pero siempre resistió. Quedó libre en marzo de 1991. El caso estimuló el análisis de nuevas leyes sobre delitos informáticos. En agosto del mismo año en que juzgaron a Nick comenzó a regir la Computer Misuse Act (Ley de Abusos Informáticos) por la cual cualquier intento, exitoso o no, de alterar datos informáticos con intención criminal se castiga con hasta cinco años de cárcel o multas sin limite. El acceso ilegal a una computadora comtempla hasta seis meses de prisión o multa de hasta dos mil libras esterlinas. El acta se puede considerar dividida en tres partes: hackear (ingresar sin permiso en una computadora), hacer algo con esa computadora hackeada (leer mensajes privados o lo que sea que constituya un delito) y realizar alguna modificación no autorizada. El ultimo apartado se refiere tanto al hacking -por ejemplo, la modificación de un programa para instalar un backdoor-, la infección con virus o, yendo al extremo, a la destrucción de datos como la inhabilitación del funcionamiento de la computadora. Pero como no hace falta hackear la máquina para modificar sus datos, bajo esta ley liberar un virus es delito. En enero de 1993 hubo un raid contra el grupo de creación de virus ARCV. Se produjeron varios arrestos en la que fue considerada la primera prueba de la nueva ley en un entorno real.

Con respecto al hacking, en 1991 la policía inglesa arrestó a Paul Bedworth, un chico de diecisiete años, bajo cargos contemplados en el acta de mal uso de las computadoras. Otros dos hackers fueron arrestados junto con él: Karl, de veintidós años, y Neil, de veintiséis, quienes se declararon culpables, esperando que eso redujera sus penas. Los abogados de Bedworth fundaron su defensa en que era un joven impresionable y que sufría de "adicción a las computadoras". El jurado lo encontró inocente, sobre la base del diagnostico de adicción presentado por el abogado. Este fue el primer caso de hacking tratado bajo el acta y, si bien logró dos condenas de tres, demostró que hay maneras de evitar el castigo. Hugo Cornwall, autor de The Hacker's Handbook, declaro que, en su opinión, el jurado estaba deseoso de dejar al chico en libertad porque el arresto había sido excesivamente violento. Sus compañeros no tuvieron tanta suerte: fueron sentenciados a seis meses de cárcel.

Holanda

Hasta el día 1 de marzo de 1993 Holanda era un paraíso para los hackers. La Galactic Hacker Party fue un ejemplo de lo que se podía hacer en Holanda sin meterse en problemas con la ley; el grupo de hackers Hack-Tic era muy bien considerado por la prensa y el publico en general, y sus relaciones con la policía eran cordiales. Pero a partir de esa fecha todo cambió. Ese día entró en vigencia la Ley de Delitos Informáticos, con artículos específicos sobre técnicas de hacking. El mero hecho de entrar en una computadora en la cual no se tiene acceso legal ya es delito y puede ser castigado hasta con seis

meses de cárcel. A partir de ahí todo empeora. Si se uso esa computadora hackeada para acceder a otra, la pena máxima sube a cuatro años aunque el crimen, a simple vista, no parece ser peor que el anterior. Copiar archivos de la maquina hackeada o procesar datos en ella también conlleva un castigo de cuatro años en la cárcel.

Publicar la información obtenida es ilegal si son datos que debían permanecer en secreto, pero si son de interés publico es legal. El daño a la información o a un sistema de comunicaciones puede ser castigado con cárcel de seis meses a quince años, aunque el máximo esta reservado para quienes causaron la muerte de alguien con su accionar. Cambiar, agregar o borrar datos puede ser penalizado hasta con dos años de prisión pero, si se hizo via módem, aumenta a cuatro. Los virus están considerados de manera especial en la ley. Si se distribuyen con la intención de causar problemas, el castigo puede llegar hasta los cuatro años de cárcel; si simplemente se escapó, la pena no superara el mes. El articulo dedicado al phreaking establece que "usar el servicio mediante un truco técnico o pasando señales falsas con el objetivo de no pagarlo" puede recibir hasta tres años de prisión. Es famosa la respuesta de un phreaker: "¿Señales falsas? ¡Yo uso solamente señales verdaderas!". La venta de elementos que permitan el phreaking se castiga con un año de prisión como tope y si ese comercio es el modo de ganarse la vida del infractor, el máximo aumenta a tres. La ingeniería social también es castigada con hasta tres años de cárcel. Recibir datos del aire es legal, siempre y cuando no haga falta un esfuerzo especial para conseguirlos; la aclaración protege datos encriptados, como los de ciertos canales de televisión setelital, aunque no esta claro qué se entiende por esfuerzo especial y todavía no hay jurisprudencia. Falsificar tarjetas de crédito o de banca electrónica y usarlas para obtener beneficios o como si fueran originales esta penado con hasta seis años, pero hacerlas y no usarlas parece ser legal.

A pesar de la ley, Hack-Tic organizó el congreso Hacking at The End of The Universe (Hackeando en el fin del universo) sin ningún problema legal; sin embargo, muchos asistentes se quejaron de que los organizadores advertían que no usaran la red instalada en el camping para hacking y casi todas las charlas se hicieron con la aclaración de que los hechos mencionados habían sucedido "mucho antes del 1 de marzo". Incluso una revista norteamericana habló del evento como "(Not) Hacking at The End of The Universe". Abogados y autoridades holandesas explicaron, en el momento de sancionar la ley, que estaba hecha para "atrapar al verdadero y peligroso criminal de las computadoras", categoría en la que incluyeron a empleados bancarios que cometen fraudes, ex administradores de sistemas que lo atacan con ánimo de venganza y traficantes de tarjetas de crédito. Sin embargo, tres semanas después de promulgada la ley, la policía de Ámsterdam arrestó al primer hacker sospechoso de infringirla. RGB, de diecinueve años, estaba usando un sistema UNIX de la Universidad Libre de Ámsterdam (Vrije Universiteit) con una cuenta que no le pertenecía. Desde esa computadora se había conectado con otra de la Universidad Técnica de Delft, por lo cual la sentencia que le correspondía en caso de que lo encontraran culpable podía llegar a ser de cuatro años. Como no quiso declarar fue detenido por treinta y ocho días pero, aparentemente en virtud de falta de pruebas, lo liberaron y no volvió a tener problemas por ese incidente.

La policía, de todas maneras, no necesitaba de la famosa ley para encarcelar a alguien. El 27 de enero de 1992, al mejor estilo del servicio secreto norteamericano, agentes holandeses entraron en la casa del hacker Wave, en Roermond, y en la de Fidelio, en Nuenen. Ambos formaban parte del grupo Time Wasters. Como sospechosos se les confiscaron equipos y diskettes y fueron transferidos a Ámsterdam,

donde permanecieron incomunicados hasta el 5 de febrero y no se les permitió ni siquiera recibir ropa de sus familiares. Se los acusó de entrar en la computadora bronto.geo.vu.nl, perteneciente a la misma Universidad Libre de Amsterdam. Falsificación de documentos, destrucción y estafa eran los cargos en su contra, de acuerdo con las leyes vigentes en ese momento, y sobre la base de que habían modificado documentos en el sistema dejándolo inutilizable (falsificación y destrucción), usando las cuentas del administrador o de usuarios legítimos (estafa). El caso no pasó a mayores, pero fue una clara advertencia a los hackers. La parte acusadora dejó pasar el límite de tiempo para presentar su denuncia y los detenidos recuperaron la libertad y sus pertenencias. Hubo quienes pensaron que el orígen de la actitud policial debía ser buscado en las presiones del gobierno norteamericano hacia el holandés como consecuencia de una infiltración en los sistemas militares de los Estados Unidos. A mediados de 1991, algunos hackers holandeses leyeron, en esos sistemas, documentos teóricamente secretos, grabaron un video y lo mostraron por televisión. Pero el gobierno de Holanda no parece estar deseoso de crear su propia operación Sundevil: hasta ahora las cosas no pasan de escarmientos o advertencias. Patrice Riemens considera que "muchas veces no es claro donde están los crímenes, ya que los involucrados -sobre todo en casos de guante blanco- no los hacen públicos para no demostrar cuan inseguros son sus sistemas. En cambio, ante un hecho de hacking se monta una gran publicidad sensacionalista con la intención de desacreditarlo porque lo que hace, justamente, es demostrar la inseguridad de esos mismos sistemas".

Chile

Chile fue el primer país latinoamericano en sancionar una Ley contra Delitos Informáticos, publicada en el Diario Oficial (equivalente del Boletín Oficial) el 7 de junio de 1993. Según ella, la destrucción o inutilización de un sistema de tratamiento de información puede ser castigado con prisión de un año y medio a cinco; como no estipula la condición de acceder a ese sistema, puede encuadrarse a los autores de virus. Si esa acción afectara los datos contenidos en el sistema, la prisión se establecería entre los tres y los cinco años. El hacking, definido como el ingreso en un sistema o su interferencia con el ánimo de apoderarse, usar o conocer de manera indebida la información contenida en este, también es pasible de condenas de hasta cinco años de cárcel (por ejemplo, utilizar una base de datos con función estadística para realizar publicidad de un producto); pero ingresar en ese mismo sistema sin permiso y sin intenciones de ver su contenido no constituye delito. Dar a conocer la información almacenada en un sistema puede ser castigado con prisión de hasta tres años, pero si el que lo hace es el responsable de dicho sistema puede aumentar a cinco. Esta ley es muy similar a la inglesa aunque agrega la protección a la información privada.

Francia

Es posible que Francia sea uno de los pocos países cuyos gobiernos sacaron provecho de la actividad de los hackers. En 1981, a poco de asumir el gobierno de Francois Miterrand, muchos franceses temerosos del socialismo sacaron del país sus capitales para radicarlos en Suiza. Un técnico descubrió cómo ingresar en las computadoras de ese país y armó un listado de más de cinco mil franceses con sus nombres reales, domicilios y todas las operaciones realizadas desde el primer día de apertura de cada cuenta. Se cree que el gobierno francés compró la información -que no pudo ser desmentida por los suizos- y tanto los infractores como los bancos sufrieron las consecuencias: devolución de capitales y

multas para evitar la prisión. Pero en 1986 se detectaron mil cuatrocientos casos de anormalidades informáticas que significaron estafas por seiscientos millones de dólares y dos años después, en enero de 1988, Francia dictó su propia Ley contra Delitos Informáticos, que prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos (mil quinientos a quince mil dólares) por "intromisión fraudulenta que suprima o modifique datos".

Argentina

En el país no hay legislación específica sobre los llamados delitos informáticos; sólo están protegidos los lenguajes de bases de datos y planillas de calculo, contemplados en la ley 11.723 de Propiedad Intelectual, modificada por el decreto 165/94, publicado en el Boletín Oficial el 8 de febrero de 1994. Si bien las modificación se realizó justamente para incluir esos ítem en el concepto de propiedad intelectual, no tiene en cuenta la posibilidad de plagio. En uno de los primeros casos que se presentaron en este sentido, el juez a cargo dictaminó que no hay jurisprudencia que permita establecer qué porcentaje de igualdad en la escritura de dos programas se considera plagio. Las copias ilegales de software también son penalizadas, pero por reglamentaciones comerciales.

A diferencia de otros países, en la Argentina la información no es un bien o propiedad, por lo tanto no es posible que sea robada, modificada o destruída. De acuerdo con los códigos vigentes, para que exista robo o hurto debe afectarse una cosa y las leyes definen cosa como algo que ocupa un lugar en el espacio; los datos, se sabe, son intangibles. Si alguien destruye, mediante los métodos que sean, la información almacenada en una computadora no cometió delito; pero si rompió el hardware o un diskette será penalizado: en ese caso, deberá hacerse cargo de los costos de cada elemento pero no de lo que contenían. Las bases de datos pueden venderse sin importar cual es la información que contienen ni para qué la va a usar el comprador. En el ámbito policial es conocido el caso de un estafador que compró una base de datos y envió una carta a cada persona informándole que había ganado un viaje por sorteo; cuando los interesados concurrían a recibir el premio les cobraba cien dólares por gastos administrativos y el viaje nunca se hacía. En cuanto a la actividad típica de los hackers, las leyes castigan el hurto de energía eléctrica y de líneas telefónicas, aunque no es fácil determinar la comisión del delito. Por ejemplo, en el caso de blue boxing -cuando se usa un número gratuito de otro país para acceder a llamadas internacionales- la dificultad radica en establecer donde se cometió el delito y quién es el damnificado. La situación varía cuando se realiza dentro del país, algo que ahora podría hacerse en la Argentina con los números 0-800 de muy reciente instalación. Por otro lado, casi no hay antecedentes de hacking interno ya que la mayoría de los organismos oficiales no tienen conexión con el exterior y tampoco están enlazados entre sí. Los pocos que están interconectados tienen un uso muy escaso, porque el espíritu que reina es el de no pasar información propia a los demás.

El comisario Juan Carlos Tirante, a cargo de la División Computación de la Policía Federal, aclara que los posibles hechos de hacking se encuadran -y afirma que en realidad son- en la categoría de delitos comunes como defraudaciones, estafas o abuso de confianza; la existencia de una computadora no modifica el castigo impuesto por la ley. El organismo nació en 1946 y tuvo su primera computadora veinte años mas tarde, pero el primer caso en el que intervino fue en el de Yuyo Barragán, en 1983. "Los hackers argentinos, por ahora -dice Tirante-, no tienen la capacidad y la tecnología que tenían sus colegas del Chaos." Para el comisario, el concepto "delito informático" califica la transgresión por su

herramienta y no por su contenido, algo poco común. El subcomisario Rubén Barreiro aclara, en un artículo de la revista Mundo policial, que la forma de denominación correcta es "delitos en informatica", ya que permite el encuadre tradicional de actos ilegales cometidos con el auxilio de una computadora. Esto podría abarcar desde delitos contra la propiedad (la mayoría) hasta delitos contra el honor (por ejemplo, incluir antecedentes falsos en archivos oficiales que perjudiquen a la persona en cuestión).

También detalla los inconvenientes con que tropiezan los investigadores en los casos donde está involucrada la informática. "Falta de legislación acorde, tanto penal como de procedimientos" y "falta de capacitación de quienes investigan" son los dos primeros puntos destacados por Barreiro. A ellos les suma "falta de cooperación de quienes deberían denunciarlos" y "ausencia de tecnología en la policía para el seguimiento de los casos". Juan Carlos Tirante explica que "la División no realiza acciones o investigaciones preventivas -al modo de las organizaciones estadounidenses-: actúa en un aspecto pericial cuando el operativo ya esta en marcha". La razón mas importante para que suceda de ese modo, según Tirante, es que "la mayoría de los delitos se cometen de la puerta de una empresa hacia adentro. Para prevenir tendríamos que estar allí y eso es como meterse en una casa para controlar que las cosas funcionen bien -imagina el oficial-; a nadie le gusta demasiado". Y nadie esta tan libre de culpas como para tirar la primera piedra. La Policía Federal adhiere, según el articulo de Barreiro, a un informe del Departamento de Justicia de los Estados Unidos en el cual se considera a una computadora como objeto (daño o robo de la máquina y/o programas), sujeto (ámbito donde se desarrolla el delito), instrumento (en general, ilícitos financieros como transferencia de valores o información falsa) o símbolo (presenta un registro falso para engañar, intimidar o conseguir alguna cesión de la víctima). El organismo acuerda, ademas, con la definición que hiciera un grupo de expertos en París en 1983 consultados por la Organización para el Desarrollo y Cooperación Económica. "Toda conducta ilegal no ética o desautorizada -dijeron los especialistas-, que implique procedimiento automático de datos y/o transmisión de datos", se encuadra en el concepto de delito informático.

Casi la totalidad de los casos en que intervino la division Computación de la Policía fueron protagonizados por empleados de las empresas afectadas -que descubrieron las fallas de seguridad en los sistemas- o por tradicionales estafadores, y no por hackers, en el sentido histórico del término. Casi todas las víctimas de delitos cometidos con computadoras, además, tratan de mantenerlos en secreto ante la pérdida de credibilidad que originaría la publicación. Juan Carlos Tirante lo menciona en su ponencia ante el VI Simposio Internacional de Criminalística que se desarrolló en septiembre de 1994 en Bogotá (Colombia) y da ejemplos claros.

A mediados de los años 80 los cajeros automáticos de un banco fueron vaciados durante un fin de semana largo. Un operador de la empresa sabía que en esos días los cajeros funcionaban off line (no estaban conectados a la casa matriz) y por lo tanto tomaban como cierta la información de la tarjeta que se presentaba y grababan en un surco especial la operación realizada. Pero si alguien tenía copias de la tarjeta podía repetir esa operación tantas veces como tarjetas tuviera. Con esta información, el operador accedió a la base de datos con los números de identificación personal de los clientes y duplicó una cantidad suficiente como para saquear los cajeros automáticos. El día siguiente al feriado las arcas del banco habían sufrido una importante merma y las autoridades tuvieron que hacer la denuncia judicial.

El operador fue detenido porque era la única persona que había preguntado acerca del funcionamiento de los cajeros.

Un conflicto gremial a finales de la misma década en una empresa mixta de capitales alemanes y del Estado argentino permitió descubrir la estafa que venía realizando desde hacia dos años la responsable del sector sueldos de la oficina personal. A raíz de la lucha por mejores salarios, los empleados de cómputos decidieron listar, de acuerdo al monto, las liquidaciones de directivos y operarios. En primer término figuraba una persona que había sido dada de baja un año antes. La responsable de sueldos sólo debió modificar un número para que se expidiera el cheque correspondiente: el nueve identificaba a quienes estaban en actividad, el cero a los que recibían la ultima liquidación y el uno a los que ya no trabajaban. Tesorería controlaba los importes pero no los nombres de los empleados. Otros ejemplos son los intentos de estafas, a través de transferencias electrónicas de dinero, contra diversos bancos del país que poblaron noticieros y páginas de diarios en el ultimo año. El primer intento se produjo el 4 de noviembre de 1993 en el Banco Francés, cuando entre siete y diez personas trataron de transferir a bancos uruguayos la pequeñez de treinta y cinco millones de dólares. Para eso secuestraron a dos supervisores del sector Comercio Exterior de la casa central bancaria y los obligaron a brindar los códigos, que pasaron a un cómplice por teléfono celular. Este controló que la operadora del sistema bancario tecleara la información correcta y se retiró convencido de haber logrado las transferencias. La estafa no se concretó por una razón en extremo fortuita: el camino de la transferencia era Buenos Aires-Estados Unidos- Suiza-Uruguay y ese día había cambiado el uso horario de la costa Este, de modo que los bancos norteamericanos estaban cerrados. Ni la operadora ni el asaltante se dieron cuenta porque la impresora que transmite los registros estaba apagada. El juez en lo Criminal y Correccional Federal Número 8, Jorge Urso, calificó la causa como "secuestro extorsivo", algo muy alejado del quehacer tradicional de los hackers.

No obstante, el intento fue suficiente como para que a los pocos días, el 11 de noviembre, se realizara el VI Congreso Argentino de Informática, en el que especialistas en seguridad brindaron conferencias a los ejecutivos de todos los bancos locales y extranjeros del país, preocupados por no convertirse en los sucesores del Francés. El uso de la informática para transferencias y operaciones de comercio exterior comenzó en la Argentina a mediados de la década del 80. Pasaron casi quince años hasta que un intento de ingreso ilegal en los sistemas bancarios se dio a conocer, pero hay que tomar en cuenta que, según la revista norteamericana Law and Order (Ley y Orden), se denuncian solo el 11 por ciento de los delitos informáticos. El FBI considera que el 85 por ciento de las intrusiones quedan impunes. Uno de los mas fabulosos robos desde la informatización de los bancos se produjo en el Security Pacific National Bank de California en los años 80. Un consultor del banco obtuvo las claves del sistema y de una cuenta con once millones de dólares transfirió casi la totalidad a un banco de Bélgica en la cuenta de un broker de diamantes, por supuesto enterado de la operación. El banco belga confirmó la operación y el consultor tuvo que esperar lo que demora el avión en llegar a Bélgica para cobrar el dinero en brillantes. La tentación de ingresar en alguna sucursal bancaria y mover dinero es grande porque también son grandes las posibilidades: tienen un promedio de trescientos mil pesos circulante. Pero en todos los casos registrados de intentos o concreción de estafas existió un empleado de la empresa involucrado en connivencia con el estafador. No es sencillo para un hacker acceder a un banco y maniobrar con las cuentas: debe saber qué tipo de máquina actúa como central del sistema, qué lenguaje utiliza y qué sistema operativo. Si tiene todos esos datos y logra acceder, todavía deberá vérselas con la base de

datos, nada simple por cierto -en general, los bancos no utilizan programas estándar, sino que desarrollan sus propios sistemas-; una vez superadas esas pruebas, el hacker quedará habilitado para hacer transferencias, cancelar saldos de tarjetas de crédito, comprar divisas, etcétera.

Gordon Morris, especialista norteamericano en seguridad informática bancaria, afirma que los sistemas en bancos y consultoras financieras son abiertos y facilitan la entrada de los hackers a través de las passwords por defecto, uno de los principales datos que aparecen en las publicaciones underground o en algunos BBSs. En los Estados Unidos los bancos están obligados a reportar al gobierno cualquier sospecha sobre un ingreso o intento no autorizado, pero las estadísticas -segun Morris- demuestran que no hay demasiados casos de infiltración de hackers. "Las transferencias electrónicas de dinero son la parte mas riesgosa de los sistemas bancarios -dice el especialista-, porque necesitan un empleado que verifique las operaciones, lo que le permite ingresar y accionar libremente. Esta situación es otra falla de seguridad, porque lo que se recomienda es que haya dos personas para activar el sistema." Morris cree que el problema fundamental radica en que los responsables no entienden realmente cuales son los riesgos, no quieren perder el tiempo y no ponen énfasis en el tema. A veces la actitud se limita a pensar que si a nadie le importa, debe estar bien. Antonio Aramouni, presidente de la Asociación de Informática Argentina, considera, por su parte, que el desarrollo tecnológico acercó al común de la gente "la posibilidad de utilizar herramientas fantásticas. Pero ¿es acaso una facilidad para el delito?", pregunta. Y se responde: "Creo que sí. Antes, para robar un banco, tenias que hacer como Mario Féndrich (tesorero del banco de Santa Fe acusado de fugarse con tres millones de pesos del Tesoro Nacional): tenías que llevarte la plata. Ahora tenés medios que te permiten robar a diez mil kilometros de distancia sin el riesgo de alarmas". Aramouni asevera que "no hay una conciencia desarrollada de la seguridad atrás de la herramienta; la gente se embelesa con la informática pero la prevención de los riesgos no tiene el mismo grado de desarrollo sostenible de la herramienta". La facilidad de comunicación entre diversos países que brinda la telemática dificulta la sanción de leyes claras y eficaces para castigar las intrusiones computacionales. El Chacal, en medio del debate por el tema, se pregunta: "Leer en una pantalla, ¿es robo? Y si salto de un satélite canadiense a una computadora en Bélgica y de allí a otra en Alemania, ¿con las leyes de qué país se me juzgará?".

VII. Usted también puede hacerlo (Manual)

We work in the dark	Trabajamos a oscuras,
We do what we can	hacemos lo que podemos,
We give what we have.	damos lo que tenemos.
Our doubt is our passion	La duda es nuestra pasion
and our passion is our task.	y la pasion es nuestro trabajo.
The rest is the madness of art.	El resto es la locura del arte.

HENRY JAMES, CITADO EN EL FAQ DE ALT.2600

Los hackers usan una gran diversidad de métodos para lograr sus objetivos, ninguno de los cuales es -como popularmente se cree- su genialidad innata ni la magia. Si se quiere entender el hacking, el primer paso es familiarizarse con las telecomunicaciones, los sistemas en general y algunos específicos. Los sistemas operativos controlan de manera absoluta el funcionamiento de las computadoras, y en su mayoría brindan ayuda extra en la pantalla, la gauchita funcion "Help". Pero hay algo más importante en este primer paso: saber sobre los sistemas aquello que no se consigna en los manuales. Las revistas constituyen una excelente fuente de información. La renombrada 2600, que edita el prócer norteamericano Emmanuel Goldstein, es una de las que brindan mayor utilidad; inclusive sus lectores que no son hackers la recomiendan. Otras ya desaparecidas, como TAP, se pueden conseguir buscando en los clasificados de 2600. Los libros acercan también datos de gran importancia. Bibliografía sobre hacking o, directamente, sobre seguridad; manuales de sistemas operativos y redes; especificaciones de protocolos; es indispensable toda aquella información que permita conocer las debilidades de un sistema y los comandos a los que responde, sus formatos de códigos, los modos de entrada y salida y cualquier detalle sobre hard y software. Los *newsgroups* (foros de mensajes públicos) de Internet, como comp.virus, alt.2600, alt.hackers, alt.security o comp.dcom.telecom -por nombrar algunos- son lugares para preguntar todo tipo de cosas y hallar la respuesta de expertos. Antes de dejar un mensaje en los newsgroups es conveniente leer las *Frequently Asked Questions* (FAQs, preguntas frecuentes) de cada uno. De cualquier modo, el arma principal del hacker es la inteligencia, pero no únicamente la suya. Para el llanero solitario de las redes, la falta de inteligencia, conocimiento o curiosidad del otro lado es

de suma utilidad. Es muy común que después de un robo espectacular se escuche la frase "Lo ayudaron de adentro". En el caso del hacker generalmente es cierto, pero no por la consciente colaboración de "el de adentro". Una password mal elegida, un sistema mal configurado, cualquier información que no siga el flujo correcto y se desvíe hacia malas manos... todo puede ser aprovechado. Si el sistema fuese perfecto no podría ser hackeado. Pero no hay sistema perfecto, siempre hay una puerta mal cerrada. El problema con el que se topan los diseñadores es que los sistemas deben ser de uso sencillo, y eso facilita el ingreso de un hacker. Si se presentan trabas no sólo los curiosos tendrán inconvenientes: los usuarios legítimos también. Si el sistema permite que el administrador acceda a los archivos secretos, el hacker que consiga los atributos de aquél va a poder usarlos.

Bichos

Cuenta la leyenda que la primera computadora digital, la ENIAC, empezó un día a funcionar mal sin motivo aparente; al revisar los circuitos, se descubrió que el problema era una polilla que se había metido en el interior del ordenador atraída por el calor de las válvulas. De allí que el termino *bug* (bicho, insecto, en inglés) haya quedado, en la jerga informática, como nombre de cualquier error de programación. Actualmente los insectos no son un problema para los circuitos integrados y los chips, pero los errores de programación siguen existiendo y se considera que un programa sin bugs es obsoleto, ya que cuando se detectaron y corrigieron todos los errores pasó demasiado tiempo desde su creación. Por lo general, un programador sabe que su producto tiene errores, pero el costo de corregirlos y enviar la nueva versión a todos los usuarios no justifica que se solucionen inmediatamente. Por eso se esperan meses, y años, hasta que las modificaciones necesarias suman una cantidad tal que imponen la necesidad de una versión actualizada. Mientras tanto, si el hacker conoce estos bugs, puede aprovecharlos. Es lo que sucedió en 1991, cuando los holandeses penetraron en el sistema del ejercito de los Estados Unidos a través de Internet. La revista 2600 lo explico así:

"Un usuario ingresa en una máquina de Internet. Usando FTP (un programa que permite copiar archivos de ida y vuelta entre dos computadoras, generalmente a través de la red) se conecta a otra, la cual pide un nombre de usuario. Tipeando 'anonymous', se obtiene un acceso limitado. El propósito es dejar disponibles archivos públicos sin tener que abrir cuentas para todos los que necesitan ingresar. Pero esta versión de FTP tiene por lo menos un gran bug en su software. Utilizando ciertos comandos (quote user ftp, quote cwd ~root, quote pass ftp) el usuario no sólo es capaz de acceder a la máquina remota sino que puede cambiar su dirección en el sistema al directorio raiz (root), la cuenta mas poderosa, que permite a quien la usa mirar todo. Además, los hackers pueden cambiar cualquier cosa, aunque con gran dificultad, porque no están realmente dentro del sistema. Todavía están confinados a trabajar dentro del programa FTP".

Un hacker habilidoso que utilice este método podrá cambiar lo que desee dentro de la máquina, incluso el archivo de passwords o agregar un usuario con los privilegios de acceso que prefiera. Por supuesto, cada vez son menos las máquinas que tienen ese bug, especialmente después de que fue publicado. Pero como dice el proverbio zen-hacker: "Es solo uno de los bugs posibles en solo una de las máquinas posibles". Otro bug típico hasta hace algunos años, que todavía se puede ver en un puñado de lugares, es el que permite entrar en la cuenta de otro después de que la persona corta. Es posible que esto suceda cuando coinciden una mala configuración del módem y bugs en el programa. En algunas circunstancias

-por ejemplo, si al usuario se le corta la llamada antes de que se desconecte- el módem puede atender otro llamado y abrir la comunicación en el punto donde quedó la anterior, adjudicando al nuevo los mismos derechos. Es especialmente peligroso si el que quedo enganchado es un supervisor: equivale a que el usuario se levante de la silla frente a su terminal y un hacker se siente en ella. Hay que caer en el momento adecuado y, como los sistemas no muestran la password, el hacker no podrá volver a ingresar en la cuenta a menos que el error se repita. Con este método, entre otros, PUA accedió a Delphi. Algunos bugs dependen de cuanto conoce el administrador las posibilidades que el sistema ofrece. El sistema operativo UNIX permite asignar a un programa, temporalmente, privilegios más altos que los del usuario. Un uso adecuado permite a un operador -por ejemplo- ingresar clientes en una base de datos, que normalmente no puede ser modificada; pero a través del programa correcto el sysop podrá agregar clientes nuevos en un banco, aunque no le sera posible cambiar el saldo de ninguna cuenta. Cuando el operador sale del programa ya no puede tocar la base de datos. Si el hacker logra acceder a ese programa, tiene que simular la salida de éste para modificar la base de datos, pero sin salir realmente, porque cuando lo hace pierde sus privilegios. Es aquí cuando un bug en el programa es crítico: si en algún momento permite ejecutar otro programa que dé la posibilidad de salir temporalmente al shell (interprete de comandos) del UNIX, el sistema continúa dándole acceso superior. Un caso común es que en algún momento haya que editar un archivo de texto con el editor Vi, que permite acceder al shell fácilmente. Una vez en el shell se puede modificar la base de datos a gusto, o, si el programa tiene suficiente acceso, crear una cuenta nueva con privilegios de supervisor. Este no es un error de programación del sistema: es un error de configuración frecuentemente cometido por los supervisores o *system programmers*.

Puerta de emergencia

Una *backdoor* (puerta trasera) permite entrar en un sistema sin usar los métodos normales. El programador puede establecerla para accesos de emergencia o para no perder el control sobre su sistema en caso de que lo maneje otra persona. Una backdoor requiere la modificación del programa, por eso en la mayor parte de los casos es obra del diseñador. De todas formas, en un sistema conocido un hacker puede crear un *patch* (parche), un programa que modifique partes del sistema para abrir una backdoor donde antes no existía. Un ejemplo clásico de esta practica es lo que hizo uno de los diseñadores del UNIX original, Ken Thompson. En una versión primitiva del sistema operativo agregó una rutina al compilador de C para que cada vez que tomara el comando "login" (el que valida a los usuarios y les dá acceso al sistema), lo modificara y permitiera ingresar a cualquiera que usara una password elegida por Thompson. Si alguien veía el código y descubría la backdoor podía sacarlo, modificando el compilador. Al advertirlo, Thompson hizo que el compilador detectara si estaba haciendo una copia de si mismo y, en ese caso, volviera a cambiar las rutinas para que la backdoor siguiera en su lugar. Por supuesto esta puerta ya no existe en las versiones actuales de UNIX.

El segundo caso, el del patch, fue usado por el Chaos Computer Club para entrar en la NASA. Introdujeron un programa en la red europea SPAN que se copiaba en todas las máquinas a las que tenía acceso. Una vez en la computadora deseada, utilizaba un bug del sistema para obtener privilegios especiales y emparchaba algunos programas para crear un usuario especial que no aparecía en los listados y era invisible para el administrador. De esta forma entraban en el sistema cuando querían.

Troyanos

Los griegos, para entrar a la ciudad fortificada de Troya, enviaron de regalo un caballo gigante de madera, con soldados ocultos en su interior. Cuando el caballo traspasó las murallas de la ciudad, los soldados salieron y la tomaron por la fuerza. En el mundo de la computación, un troyano es un programa que parece una utilidad pero no lo es; el usuario lo ejecuta confiado, porque cree en las especificaciones, y se ve sorprendido en su buena fé. Un ejemplo típico es un programa que dice servir para hacer trampa en un juego, pero que cuando se pone en marcha destruye el disco rígido. En 1987, en Alemania, se registró un inocente caballo de Troya: se llamaba Christmas (Navidad) y el operador debía teclear esa palabra para que en su pantalla se dibujara un típico arbol adornado; mientras tanto, el programa leía la agenda electrónica y se enviaba a si mismo a todos los teléfonos que encontraba. Corrió por European Academic Research Network (EARNet, Red de Investigaciones Académicas Europea), BitNet (red con mil trescientas sedes en los Estados Unidos), VNet (correo electronico privado mundial de IBM) y cuatro mil computadoras centrales, mas las personales y estaciones de trabajo. A los dos días se paralizó la red de IBM.

Hay formas mas sutiles y menos dañinas de hacer troyanos. Un hacker podría reemplazar el login de UNIX, por ejemplo, por un programa que haga exactamente lo mismo pero guarde una copia de la password ingresada por el usuario en un archivo accesible para él. Login es la pantalla que muestra un sistema cuando alguien intenta ingresar; en general consta de dos elementos: el pedido de identificación (username, login, ID) y la solicitud de clave o password. Si el hacker tiene interés en algún archivo en particular al cual no tiene acceso, puede enviarle al supervisor un programa disfrazado de juego que, al ser ejecutado, copie ese archivo en un lugar accesible. Si están bien hechos, los caballos de Troya no son fáciles de descubrir, aún por un administrador experimentado; The Knightmare aconseja en su libro Secrets of the Superhacker tomar algunas precauciones en el momento de diseñarlo: que no acceda al disco rigido o periféricos porque llamaría la atención del operador; distraer a quien lo ejecuta con algún mensaje o nota en pantalla; no utilizar comandos que -en caso de ser revisados manualmente por el administrador- demuestren el real objetivo; no colocarlo al principio ni al final del archivo.

Señuelo

Un *decoy* (señuelo, en ingles) es un programa diseñado para que el usuario caiga en un movimiento donde se le pueda robar la password. Si un hacker tiene cuenta en una máquina o servicio determinado y quiere sacarle la password al administrador, puede conectarse con su cuenta y dejar un programa que imite al login normal de la computadora; se desconecta y espera a que el sysman entre al sistema usando su programa. Cuando éste ingresa nombre y password, el decoy -segun su implementación- puede por ejemplo anunciar que hubo un error y presentar el login verdadero, o puede hacer el login por él: en cualquier caso, el administrador no notará nada raro. Otro método es poner en el ordenador que se quiere hackear un programa que guarde todas las teclas que se presionan, algo bastante común en DOS. De esta manera, el hacker puede leer lo que el usuario tipeó, incluyendo passwords, programas de acceso o tráfico de información. Instalando uno de esos programas en una máquina que sea puente de una red, como un PAD, el hacker puede conseguir direcciones interesantes dentro de esa red, inclusive las passwords que se registren en ese nodo.

También se puede montar un sistema falso para que la víctima se conecte pensando que ingresa en el lugar original: tal es lo que hicieron Doctor Trucho y El Chacal para averiguar el NUI de otro hacker. Por lo general, estos programas muestran un login igual al del sistema verdadero y luego de que el usuario teclea su password responden con algún tipo de error para que salga del sistema. Si se trata de una terminal a la que el hacker tiene acceso físico, se pueden cambiar los cables y conectarlos a otra máquina. Si es por teléfono, puede convencer al usuario de que el numero telefónico cambió (algo desaconsejable, porque si el usuario sospecha puede pedir confirmación) o, si la compañía telefónica lo permite y el hacker se las ingenia, puede redirigir la línea verdadera a un aparato elegido por él.

El Adivino

Para acceder a una máquina de la que se conoce el nombre de una cuenta (como *root* en UNIX) pero no la password, una posibilidad es probar todas y cada una de las combinaciones para conseguirla. El método se conoce como *fuerza bruta* y no es nada sencillo. Si el sistema permite letras de la A a la Z, mayúsculas y minúsculas, ademas de números del 0 al 9, y un largo de ocho caracteres, las posibilidades de comparación son 218.340.105.584.896, sin contar teclas especiales y siempre que todas las passwords sean exactamente de ocho dígitos. Probando un millón de combinaciones por segundo se tardarían casi siete años. Si se tiene en cuenta que algunos sistemas obligan al usuario a esperar unos segundos entre cada intento de login erróneo, es fácil sospechar que tal vez no se trate del acercamiento más práctico a la solución. Pero los sistemas son usados por personas, no por abstracciones matemáticas. Eso permite pensar caminos más cortos: muy poca gente, por ejemplo, va a elegir recordar una password como "Hks4Ijdh"; normalmente se prefieren claves como "Gustavo", "Mnemonic", "aeiou" o cualquier otra fácil de retener en la memoria. En particular es muy común el uso del mismo nombre de login como password: si el usuario ingresa como "pepe", es probable que su clave sea "pepe". Un estudio realizado en la Universidad de Míchigan reveló que cinco de cada ochenta usuarios escogen como password su nombre. También es frecuente el uso de una sola letra, con lo cual las posibilidades se reducen a cincuenta y dos, contando mayúsculas y minúsculas. Un usuario puede elegir como contraseña el nombre del sistema o, por ridículo que parezca la palabra "password". En términos generales, nombres de personas, animales, lugares, marcas y personajes de ficción son elecciones muy comunes. Esto reduce el espectro, aunque sigue siendo muy grande.

Un programa, el Password Cracker, permite chequear automáticamente las passwords corrientes. Es raro que se lo use contra un sistema en tiempo real: la mayoria de las veces se consigue el archivo encriptado de passwords y se chequea contra el programa. Las claves están encriptadas con un algoritmo de una sola dirección, aquellos que permiten encriptar un texto pero no desencriptarlo. Es decir, no hay modo de conseguir la password a partir del archivo. Para chequear si la password ingresada por el usuario es correcta, el sistema encripta la clave que ingresa y la compara con el archivo. Un hacker que tenga un archivo de contraseñas puede tomar una palabra, encriptarla y ver si está en ese archivo. En UNIX el archivo de contraseñas es legible por cualquiera y en muchos sistemas se puede conseguir a través del FTP anónimo. Los programas chequeadores pueden verificar setecientas passwords por segundo si la computadora es una 486: cada palabra es encriptada en un diccionario (preparado por el hacker) y la chequean contra todas las passwords del archivo. Se puede adivinar un veinte por ciento de las claves en cuestión de horas o, si se usan diccionarios grandes, en un día. Este método no descubrirá contraseñas como "PdejkK", pero va a encontrar las más comunes. La

defensa mas usada para evitar esta técnica es permitir pocos intentos y desconectar la computadora si no se ingresa una password correcta. Otra posibilidad es buscar cuentas sin passwords, o passwords default.

Cuando los hackers saben que en un sistema determinado el usuario "admin" viene configurado con password "admin", es lo primero que prueban. En general sucede con los que no son demasiado usados, como una cuenta para mantenimiento de emergencia, que puede llamarse "admin2" y no tener password por default. El administrador puede haber olvidado corregirlo y hasta puede ignorar que existe. Leer el manual del sistema con detenimiento permite vislumbrar posibilidades que, tal vez, el supervisor no conoce. También pueden aprovecharse los procesos automáticos. En una red es probable que exista un usuario "backup" sin password, o con una obvia como "backup", que sólo se utilice para realizar una copia de seguridad al ingresar. Este proceso debe acceder a todos los archivos por razones obvias; es, en consecuencia, un blanco apetecible para un hacker que puede usarlo si se conecta con ese nombre, aborta el backup y logra quedar en un shell de comandos.

Otras cuentas con menos prioridades permitirán ingresar en el sistema con privilegios mínimos y usar diversos métodos para aumentarlos. En una red Lantastic, un usuario accedió con la cuenta "clock", que servia para sincronizar los relojes de las máquinas y no tenía password ni acceso a casi nada; luego usó un programa del sistema mal configurado que le permitía ver lo que estaba haciendo otro usuario en otra terminal.

Si de adivinar passwords se trata, siempre es útil saber lo mas posible sobre el usuario en cuestión. The Knightmare cuenta que un fanático de Popeye tenia como password "OliveOyl"; en la película Juegos de guerra la clave era el nombre del hijo de quien había diseñado el sistema. Averiguar datos del usuario es de gran utilidad, pero las posibilidades de hacerlo dependen del objetivo: si el hacker tiene acceso al lugar y puede hablar con los empleados, algunas preguntas bien hechas pueden ayudar. "¿Cuál es tu password?" revelería sin más las intenciones y una persona que se interesa por los nombres de amigos, novias, animales y parientes puede resultar sospechosa. Pero si alguien se para en la puerta de un edificio y reparte cuestionarios para una supuesta encuesta, nada llamará la atención y quizá obtenga las respuestas necesarias. Si bien ningún sistema muestra en pantalla la password mientras se la tipea, una vista rápida puede seguir el movimiento de los dedos y descubrir qué letras marco el usuario: la técnica se llama shoulder surfing y consiste en el antiguo truco de mirar discretamente por sobre el hombro del otro. Muchos hackers disimulados supieron conseguir interesantes datos frente a teléfonos públicos, por ejemplo: claves de servicios de llamadas de larga distancia.

Los programas de comunicaciones también son una fuente de passwords. Algunos, como el Terminate, permiten guardar la clave del usuario junto con el teléfono del sistema. Otros dejan realizar "scripts", programas que facilitan la comunicación con determinados lugares, en los cuales seguramente esta la password sin encriptar. Conseguir una contraseña de esa manera requiere acceso físico a la computadora o, a través de una red, al directorio donde se hallen.

¿Mi password? Como no

La mejor fuente de información sobre un sistema son los usuarios. Muchos NUIs de Arpac fueron robados llamando a una empresa con cuenta en esa red y preguntándole la password a algún empleado. Por supuesto hay que justificar la necesidad de pedir esa información. El método se llama *social engeenering* y consiste en convencer a la gente de que debe informar algo que teóricamente no corresponde. Fry Guy lo usó para obtener los datos que le permitieron hackear la agencia de crédito CSA, pero hay miles de casos que lo ejemplifican. Emmanuel Goldstein cuenta que un hacker llamó a una empresa y preguntó el numero de teléfono para acceder a su computadora. Habló con el responsable del centro de cómputos pasando por un usuario legítimo, pero ante las sospechas del operador se puso nervioso y dió respuestas contradictorias. El hombre amenazó con denunciar de inmediato ese intento de ingreso ilegal al administrador del sistema. El hacker consultó con otro colega, quien lo tranquilizó: "No te preocupes, yo voy a arreglar todo", fueron las palabras. Dejó pasar media hora y se comunicó de nuevo con el operador. "Buenas tardes. Le hablo de la oficina del administrador del sistema -mintió-. Usted denunció hace unos momentos un intento de averiguar el número de acceso a nuestra red; hizo un gran trabajo, lo felicito. Para confeccionar el informe necesito que me diga cual es el número que querían averiguar".

El operador se lo dio, el hacker agradeció y colgó: habían obtenido el numero aún después de que parecía imposible. Esta técnica puede adoptar muchísimas formas y se puede realizar por teléfono, personalmente, o por escrito. Por ejemplo, es posible que alguien simule ser inspector de la Dirección General Impositiva (DGI) y vaya a la empresa cuya computadora se quiere hackear para ver los archivos: la persona que atienda al truchinspector tendrá que brindarle la contraseña para acceder a la información contable. También es posible fingirse periodista y preguntar con profesional inocencia todo sobre el funcionamiento del sistema de una empresa. Son formas indudablemente peligrosas: permiten que luego el hacker pueda ser reconocido. Por escrito se puede solicitar a las empresas, usurpando el lugar de un usuario, información sobre los errores de los programas o sobre su funcionamiento.

Cartoneo Informático

Los diagramas de flujo de la información terminan típicamente en un mismo punto: el archivo. Una factura, una orden de compra, un listado de números telefónicos de acceso a una red se guardan en una caja hasta que alguien necesita verlos. Pero no toda la información que circula en una organización sigue un diagrama de flujo correctamente diseñado. Un operador puede anotar su contraseña en un papelito y una vez que se la acuerda de memoria tirarlo a la basura. Uno de los principios de la termodinámica dice que nada se destruye, todo se transforma: el papelito con la información comprometedora va a salir de la organización en una bolsa y Manliba se ocupará de ella. Desde que sacan la basura de la empresa hasta que pasa el camión de Manliba, un hacker puede revisar la bolsa y encontrarlo. Esta técnica se llama *trashing*, del ingles trash, basura. Bruce Sterling concurrió a una reunión de agentes norteamericanos federales durante la investigación que realizó para su libro The Hackers Crackdown. Mientras esperaba fuera de la sala de conferencias se preguntó que haría un hacker en esa situación: buscaría entre la basura cualquier dato de valor. Decidió husmear en el cuarto de enfrente, que no tenia relación con los investigadores. Entre los papeles de la basura encontró una

cuenta telefónica de larga distancia de Sprint a nombre de Evelyn. Un cartel escrito en computadora decía: "Trata a tu tarjeta de teléfono como a cualquier tarjeta de crédito. Para asegurarte contra un fraude, nunca digas tu numero por teléfono a menos que tú hayas llamado. Si recibes llamados sospechosos notifica a servicio al cliente inmediatamente".

Sterling pegó los pedazos con cinta adhesiva y pudo ver los diez dígitos de identificación de la tarjeta aunque faltaba el código, pero tenia el teléfono de Evelyn y los de muchos de sus amigos en el mundo. Si Sterling hubiera sido un hacker habría tenido gran cantidad de información para explotar. Un papel con una palabra anotada puede ser una contraseña, pero quizá no sirva demasiado si no se sabe a quién pertenece; un cuaderno con notas tomadas en algún curso puede ser una caja de Pandora. Es posible que el alumno anotara en detalle los pasos para entrar en un sistema y aún a falta de contraseñas esa información servirá para saber cómo funciona ese sistema. Y no sólo de papelitos cartoneados vive el hacker: no hay que olvidar los manuales. Muchas veces las empresas compran diez paquetes de software porque la ley de copyright les impide instalar uno solo en todas las máquinas. Cada paquete trae su manual respectivo y, como suelen ser voluminosos, no es improbable que los empleados, una vez que crean dominar el sistema, los tiren. Recoger uno significa acceder a información difícil de conseguir sin comprar el producto. Un memorándum interno que explica procedimientos de seguridad, o detalla números de acceso externos al sistema de la compañía es invalorable. El riesgo del trashing es que alguien vea al hacker cuando lo está haciendo y pida explicaciones. The Knihtmare sugiere en su libro decir que se están buscando latas para reciclar.

En la Argentina esta excusa no es demasiado creíble, pero hacerse pasar por botellero es sencillo si se consigue un carrito y se toma la precaución de vestirse adecuadamente. Todo lo que se encuentre en la basura es potencialmente útil si el hacker sabe cómo usarlo y darle el significado correcto, al mejor estilo Sherlock Holmes.

La Infección

Pocas cosas en el mundo informático excitan más la imaginación popular que un virus. Son programas que aparentan tener vida propia y que invaden las computadoras sin permiso. Se duplican a sí mismos y suelen tener lo que se llama el *payload*, el código que infecta al sistema. Este puede ser inofensivo -los hay que meramente muestran un mensaje- o destructivo; en cualquier caso es peligroso ya que, como mínimo, ocupa espacio en el disco y en la memoria. El primer caso conocido sucedió en 1960. "El monstruo de la galletita" -como fue bautizado el virus pionero en un articulo de la revista norteamericana *Time*- solo se ejecutó dentro de una universidad. Presentaba por toda actividad una leyenda en la pantalla: "I want a cookie" ("Quiero una galletita"); no se reproducía; solo se repetía hasta trabar la maquina. La forma de desactivarlo era sencilla -aunque en la desesperación hubo quienes probaron métodos extraños, desde preguntar que tipo de galletita hasta acercar una al ordenador-: había que teclear la palabra "Cookie". ¿Por que no darle lo que pedía?. Un virus parece el hacker ideal, pero no es tan cierto. Es un ente ubicuo y puede estar en cualquier parte, pero no es una ventaja para el hacker: no siempre va a aparecer donde le interesa. Un virus se escapa de control demasiado rápido y no se puede usar fácilmente para atacar a un sistema en particular.

Unicamente es perfecto para el vandalismo indiscriminado. Según la definición mas aceptada, se trata de un programa que modifica a otros agregándoles su código y -de esa forma- reproduciéndose. El

doctor Fred Cohen, el primer estudioso reconocido de los virus, tiene su propia definición: un virus es cualquier programa que se autorreproduzca. Según el, un gusano -un programa que no modifica a otros para reproducirse- también es un virus. La diferencia consiste en que estos se ejecutan cada vez que el usuario utiliza el programa infectado mientras que los gusanos deben buscar otros métodos, pero el uso de ambos en el hacking es similar: si es el objetivo, tanto unos como otros envían de regreso la información que recolectan. Por lo general un virus se copia en un diskette, de allí pasa de máquina en máquina y se pierde el control de donde va. Si un hacker quisiera usarlo debería asegurarse de que ataque a la máquina correcta, para lo cual un virus normal de DOS no serviría. Necesita un virus programado especialmente para redes, que busque el camino desde su punto de origen hasta la víctima.

El gusano de Morris es un ejemplo excelente: aunque el no buscaba atacar a un sistema en particular, usaba algunas técnicas de hacker para copiarse a lo largo de Internet. Otro ejemplo es uno de los experimentos de Fred Cohen, quien consiguió permiso para probar su virus en un sistema operativo que usaba una técnica llamada Bell-LaPaluda que, se suponía, estaba diseñada para dar un grado máximo de seguridad e impedir la filtración de información. La idea de Fred era demostrar que un usuario con privilegios mínimos podía introducir un virus para que accediera a la información mas clasificada. El programa que Cohen desarrolló tuvo éxito: el secreto es que si un usuario con bajo nivel de acceso infecta uno de sus programas y consigue que otro de mayor privilegio lo ejecute, el virus va a tomar automáticamente los derechos del segundo y así hasta llegar al máximo nivel. Para que funcione hay que tener acceso al sistema para, por lo menos, ingresar el virus. La clave consiste en saber que el programa es el usuario (sea un virus o no, tiene el mismo nivel de acceso que el usuario). Si el supervisor lo ejecuta, podrá acceder a todo el sistema y una vez alcanzado ese nivel puede hacer lo que el hacker quiera: filtrar información secreta, instalar un backdoor o cualquier otra cosa.

Búsqueda Frenetica

Scanning (busqueda) es, en el argot del hacker, la revisión de una serie de posibilidades dentro de un sistema -por ejemplo, una red- para encontrar datos interesantes. Es el discador tipo Juegos de guerra: un programa llama mediante un módem a un numero telefónico tras otro y chequea que conteste otro módem. Guarda en un archivo los que encontró (incluso, según el software, el cartel de bienvenida al sistema alcanzado) para que el hacker luego lo analice con tranquilidad. Puede hacerse a mano si se buscan Private Branch Exchanges (PBX, centrales telefónicas internas de empresas), donde un módem no es útil. La desventaja es que, dada la cantidad de números telefónicos existentes, lleva demasiado tiempo, por lo que su práctica se reduce a una cantidad menor, como los publicados en guía de una empresa determinada. Pero una vez conseguido el dato se puede manejar el circuito telefónico interno y utilizarlo para salir al exterior con llamadas de larga distancia. La técnica no está limitada a la red telefónica: se puede hacer scanning de números IP (la identificación de la máquina) en una red TCP/IP (como Internet) o intentarlo con ondas de radio. Muchos equipos de radio vienen preparados para buscar automáticamente señales dentro del espectro radial que reciben. El hacker puede escuchar y obtener información interesante: llamadas telefónicas por inalámbricos y celulares, comunicaciones de fuerzas de seguridad, etcétera. Toda la información que viaja por el aire está a disposición del hacker para ser analizada, desde cables de agencias de noticias hasta mensajes para los servicios de radiollamadas. Claro que algunos de estos datos requieren un equipamiento especial -disponible y a la venta en los Estados Unidos y otros países- para ser detectados.

Cajitas

Para manipular las lineas telefónicas, phreakers y hackers inventaron una serie de dispositivos llamados "cajas". La mas conocida es la Blue Box (Caja Azul), un aparato que emite un tono de 2600 hertz con el cual convence a la central telefónica de que un operador u otra oficina de la empresa esta usando la línea. Quien opere una Blue Box puede controlar a gusto una central: hacer llamadas gratis, redirigirlas y todo lo que permita el software que la controle. Otra caja popular es la Black Box (Caja Negra), que evita que la central telefónica detecte que el auricular fue levantado. Impide el cobro de las llamadas hechas a un teléfono equipado con este aparato. Una Red Box (Caja Roja) emite tonos equivalentes a los que envían a sus centrales los teléfonos públicos de los Estados Unidos, simula que se ponen moneadas y, en consecuencia, la comunicación resulta gratis. Una Cheese Box (Caja de Queso) dirige las llamadas de un teléfono a otro; el Infinity Transmiter (Transmisor Infinito) permite escuchar las llamadas hechas al teléfono donde esta instalado.

Celulares

Los teléfonos celulares son especialmente vulnerables al hacking: sus chips pueden ser reprogramados para presentar el código de un llamador falso y evitar el pago. En general, la gente cree que impiden que la policía pinche las lineas, por eso lo prefieren -entre otros- los distribuidores de drogas, aunque es un error: no están libres de que alguien escuche sus conversaciones, tal como lo demostraron los hackers argentinos en el Congreso de 1994. En sus orígenes, los aparatos traían el numero de serie en un chip de memoria, lo que permitía reprogramarlo y cambiarlo a uno pirata. Ahora ese numero esta dentro de un chip que no es programable. En 1993 los países con mayor cantidad de fraudes cometidos por via celular fueron República Dominicana, Egipto, Pakistán, India, Rusia, El Salvador, China, Colombia, México y Ghana. En 1993 la agencia de créditos TRW anunció una técnica de "firma" que debe coincidir con el número de teléfono y el de serie, pero los conocedores del tema aseguraron que es un parche.

El ingeniero Armando Parolari trabaja en la actualidad para la empresa de telefonía celular CTI. Afirma que "se pueden usar todas las líneas, porque si alguien se dedica a enganchar una frecuencia libre puede usarla, pero creo que el sistema celular es el mas confiable, porque tiene que ser algo muy circunstancial". Parolari está convencido de que la telefonía celular sera la forma de comunicación del futuro, porque ofrece una ventaja que considera imbatible respecto de las de cable rígido: la comodidad de llevar consigo el teléfono. Para apoyar su teoría asegura que "hay países nórdicos que tienen un desarrollo de sistema celular equivalente al que nosotros tenemos en telefonía fija, es decir seis abonados por cada seis habitantes", pero reconoce que la gran limitación es la banda de frecuencia. Opii no comparte la opinión de Parolari sobre la mayor seguridad de la telefonía celular. "Eso es una broma, el que dijo eso es un nabo -define, contundente, el chico- no tiene idea de nada. Es muy fácil, con modificar el televisor, ya está. Tenés que recibir una determinada banda de frecuencia: entre 800 y 900 MHZ están los teléfonos celulares. Con cualquier cosa que reciba en esa banda, podes escuchar las conversaciones. Después, si querés captar o usar uno en especial, es mas complicado. Pero escuchar, lo hace cualquier estúpido."

Digitales

En cuanto a los medios digitales, en este momento hay por lo menos tres CD-ROMs con información sobre hacking que se consiguen fácilmente. Los CD-ROM “BBS underground” contienen archivos con materiales que van desde programas para hackear hasta instrucciones precisas para hacer determinadas operaciones. Conseguir sus números telefónicos no es difícil: en los BBSs corrientes hay listas de otros y, una vez que se accede a uno, descubrir más es sencillo. Los operadores no se preocupan por mantener cautiva a su clientela y, en general, reservan un centro de mensajes o de publicidad donde figuran los teléfonos.

Un BBS es un programa que funciona con el módem de la computadora y que permite a quien llama elegir opciones desde una pantalla o menú principal. Las principales son: correo; envío y recepción de archivos con diversas informaciones, programas o materiales publicados en otros medios; en algunos casos también hay juegos y se puede mantener una conversación on line con el operador. Algunos son abiertos y cualquiera puede ingresar y accionar; otros son absolutamente cerrados y se limitan a presentar información, no admiten respuestas. Están los anónimos (el operador no sabe el nombre ni el domicilio de los usuarios), intermedios (el sysop conoce la identidad de los usuarios pero estos no la de los otros usuarios) y los que prohíben el uso de seudónimos; los públicos y gratuitos; los privados (casi siempre cobran por asociarse y restringen los usuarios a amigos del operador). Algunos marcan status entre sus usuarios y, por ejemplo, no permiten el acceso de niños a determinadas áreas. Aunque no se trata de algo cotidiano se puede hackear un BBS, pero hay muchos que no cobran por el servicio y hacerlo solo servirá para recolectar información acerca de los usuarios y sus claves. Los de mayor tamaño, generalmente masivos, nacionales y comerciales, que ademas brindan servicios on-line -como Compuserve o Delphi- son, tradicionalmente, objetivos para el hacking. Los importes que cobran por asociarse resulta casi siempre elevados, pero contienen datos que los hackers saben utilizar.

En cuanto a las *redes*, en la actualidad la única que se tiene en consideración es Internet: a través de ella es posible llegar a otras treinta mil redes y a dos millones y medio de computadoras diseminadas por el mundo. Para un hacker que da sus primeros pasos es conveniente entrar en el underground y relacionarse con gente que esté en el tema.

En la práctica, sin embargo, resulta muy difícil limitarse a usar los conocimientos de otros. Compartir descubrimientos, técnicas, e información es una de las mas antiguas tradiciones dentro del mundo hacker, pero no significa que los secretos se revelen indiscriminadamente: es necesario ganarse la confianza de los hackers mas avezados y demostrar que el interés esta en adquirir conocimientos y no en conseguir llamadas de larga distancia gratis sin saber cómo. Los grupos de hackers suelen ser bastante cerrados y desesperarse por ingresar en ellos puede cerrar las puertas; las chances aumentan si se puede demostrar que se tiene algo para ofrecer y que se es una persona confiable y discreta.

Los responsables de la seguridad de los sistemas son conscientes de todas estas posibilidades y por lo tanto, toman precauciones. Una de ella es instalar un "*cortafuegos*": una computadora que registra todos los paquetes de información que ingresan en la compañía para, una vez verificados, derivarlos a otra que tiene conexión interna y no recibe archivos que no provengan de aquella. En el camino inverso, la interna envía los datos a la máquina que tiene conexión con el exterior y ésta no acepta paquetes que registren otro origen. Los directivos de seguridad de AT&T instalaron un cortafuego en la

oficina central de la compañía para preservar el sistema y Marcus Ranum, del Trusted Information Systems, diseñó uno para la Casa Blanca. A veces se instala un *ring back*: el que llama debe ingresar una identificación correcta, luego la computadora corta la conexión y llama al teléfono registrado para ese usuario. Pero así como surgen nuevas medidas de control, nacen nuevas ideas para hackear: por ejemplo, el ring back se burla levantando el teléfono y simulando un tono de linea desocupada para que el módem piense que está marcando el numero, pero en realidad sigue conectado con el que llamó. El rango de cosas que el hacker puede estudiar es inmenso: ningún detalle puede de manera alguna agotar el vasto campo de exploración posible.

Pequeño Hacker Ilustrado

+ **Administrador** : persona que se encarga de todas las tareas de mantenimiento de un sistema

+ **ARPAC** : red argentina de packet switching, norma X.25.

+ **ASCII** : American Standard Code for Information Interchange. Código de representación binaria de numeros y letras.

+ **Backdoor** : puerta de entrada trasera a una computadora, programa o sistema en general. Sirve para acceder sin usar un procedimiento normal.

+ **Backup** : cualquier cosa que sirva para restaurar un sistema ante un desastre. Pueden ser cintas o diskettes que contengan la información que hay en el sistema. También cualquier cosa que sirva para reemplazar a un elemento defectuoso. Una línea telefónica backup, por ejemplo, está para cuando la que normalmente se usa deja de funcionar.

+ **Bajar** : recibir un archivo por módem de un host.

+ **Base de datos** : se utiliza como sinónimo de BBS, pero en realidad es cualquier conjunto de datos organizados.

+ **BASIC** : Beginner's All Purpose Symbolic Instruction Code (código simbólico de instrucciones de todo propósito para principiantes). Lenguaje de programación sencillo de instrumentar y de aprender, que se uso mucho en las primeras computadoras personales. Tiene muy mala prensa porque lleva a sus practicantes a vicios de programación.

+ **BBS** : Bulletin Board System (sistema de boletines). Es una computadora con un módem y con un programa que atiende cada vez que alguien llama con otro módem por teléfono. Presenta al usuario un menu de actividades. Las más comunes son la transferencia de archivos y correo electrónico.

+ **Bit** : Unidad mínima de información. Equivale a un 0 o a un 1, a un si o a un no. Combinando bits se puede representar números, palabras, dibujos, sonidos, etcétera.

+ **Black Box** : aparato que engaña a la central telefónica haciéndole creer que no se levanto el tubo del teléfono cuando en realidad se está produciendo una comunicación.

+ **Blue Box** : aparato (o programa de computadora) que emite tonos multifrecuencias que permiten controlar las centrales telefónicas. Se usa para lograr comunicaciones gratuitas, entre otras cosas.

+ **Bps** : bits por segundo. Medida de velocidad de transmisión de un módem.

+ **Bug** : un error en un programa o en un equipo. Se habla de bug si es un error de diseño, no cuando la falla es provocada por otra cosa.

+ **Byte** : ocho bits. La unidad minima de información que puede procesar una computadora de una sola vez. Si tomamos al pie de la letra la definición, no todos los bytes tienen ocho bits, porque algunas computadoras manejan 7 bits, otras 9. Pero por lo general un byte son ocho bits.

+ **Calling Card** : tarjeta de crédito emitida por una compañía telefónica que permite comprar crédito telefónico e irlos debitando al hacer llamados.

+ **Carding** : arte de abusar de tarjetas de crédito.

+ **Chat** : charla en inglés. Se aplica cuando un usuario de una red o de un BBS habla con otro en tiempo real a través del módem o lo que sea que maneje la red.

+ **CIBA** : Central Internacional Buenos Aires. Central telefónica para llamadas internacionales, usada en los 80. Por extensión, se llamaba CIBA al nodo Telenet/Tymenet que se instaló en dicha central.

+ **Ciclos** : cantidad de oscilaciones por segundo. Se aplica a las (por segundos, HZ) oscilaciones de sonido, pero también describe todo tipo de oscilación.

+ **Clave** : se usa como sinónimo de password; tambien puede ser el código que permite desencriptar un dato.

+ **Código fuente** : programa escrito en Pascal, C, Basic, o cualquier lenguaje. En ese formato no es entendible por la computadora; necesita ser "traducido" (compilado) para que lo entienda.

+ **Colgar** : a) hacer que un sistema deje de funcionar; b) desconectar una comunicación telefónica.

+ **Compilador** : programa que toma el código fuente de un programa y lo convierte a un ejecutable.

+ **Configuración** : conjunto de las opciones elegidas por un administrador para un sistema.

+ **Correo electrónico** : equivalente electrónico al correo normal en el que se intercambian mensajes entre dos (o mas) personas, a través de una red o de un BBS.

+ **Correr** : sinónimo de ejecutar.

+ **Cortafuegos** : computadora que registra todos los paquetes de información que entran en una compañía para, una vez verificados, derivarlos a otra que tiene conexión interna y no recibe archivos que no provengan de aquella.

+ **Cracker** : a) persona que quita la protección a programas con sistemas anticopia; b) hacker maligno,que se dedica a destruir información.

+ **Cuenta** : darle a una persona acceso a una red, a un sistema o a un BBS. Como su homónima en el banco, consiste en los datos personales de un "cliente" (en este caso, cliente de un sistema) que permiten que este use los servicios ofrecidos. Por lo general se identifican con un nombre.

+ **Cyberespacio** : la "alucinación consensuada" de Gibson. Es el conjunto de todas las redes, que forman un "espacio virtual".

+ **Cyberpunk** : corriente literaria dentro de la ciencia ficción que, entre otras cosas, se destaca por incorporar a sus argumentos el uso de la tecnología de las redes de computadoras.

+ **Decoy** : señuelo en inglés. Programa diseñado para que el usuario caiga en un movimiento donde se le pueda robar la password.

+ **Default** : si un programa presenta al operador varias opciones y permite que no elija alguna en particular, utiliza una de estas como la respuesta mas general. Esto se llama opción default, por defecto, ya que el usuario no eligió nada.

+ **Dial-Up** : línea de datos que permite a un usuario ingresar por módem a una red o a una computadora.

+ **DDI** : Discado directo internacional.

+ **Discador** : aparato que sirve para discar por teléfono, o programa que usa dicho aparato. Por lo general se trata de un módem, o un programa que lo usa.

+ **DOS** : Disk Operating System (sistema operativo de disco). Es el sistema operativo que mas usan las PC compatibles con IBM. También es el primero que se hizo para ellas.

+ **E-mail** : correo electrónico.

+ **Ejecutable** : un programa listo para ser ejecutado por la computadora

+ **Ejecutar** : interpretar las instrucciones de un programa y llevarlas a cabo.

+ **Encriptar** : codificar un dato de forma que sólo pueda ser leído por el destinatario.

+ **FAQ** : lista de preguntas frecuentes, con sus respuestas, aparecidas en un determinado newsgroup.

+ **Fidonet** : red de BBS internacional. Están conectados por teléfono, es gratuita y estrictamente no

profesional.

+ **FTP** : File Transfer Protocol, protocolo de transferencia de archivos, sistema para copiar archivos a través de Internet.

+ **Guest** : cuenta pública en un sistema, para que la use alguien que no tiene una cuenta propia.

+ **Gusano** : programa que se reproduce, sin modificar a otros en el intento.

+ **Hacker** : este libro trata de definir esta palabra.

+ **Handle** : seudónimo usado por un hacker en lugar de su nombre verdadero. También se usa entre los radioaficionados.

+ **Handy** : radio receptor y transmisor de mano.

+ **Hang-up** : véase "colgar" acepcion "b".

+ **Hardware** : todo componente físico de la computadora.

+ **Host** : computadora que es "huésped" de otras, en una red. Puede que les ofrezca espacio en disco, programas, un impresora, o cualquier servicio.

+ **ID** : identificacion

+ **Ingenieria social** : arte de convencer a la gente de entregar información que no corresponde.

+ **Internet** : red de redes. Une máquinas de distintas tecnologias, sistemas operativos y fabricantes, con un protocolo común. No es una organización, no tiene líderes ni dueños.

+ **IUR** : Identificación de usuario de red. Castellanización de NUI.

+ **Kilobyte** : 1.024 caracteres.

+ **Lamer** : tonto, persona con pocos conocimientos o con poca "etiqueta".

+ **Login** : procedimiento de identificarse frente a un sistema para luego usarlo.

+ **Loops** : circuitos. Un loop de teléfonos son dos teléfonos que se comunican entre si.

+ **MaBell** : nombre cariñoso con el que se llama a la Bell Corporation o a cualquiera de sus empresas

subsidiarias.

+ **Mainframes** : computadoras grandes. A diferencia de las personales, ocupan habitaciones enteras y tienen un gran número de terminales.

+ **Megabyte** : 1.024.000 caracteres.

+ **Módem** : MOdulador DEModulador. Aparato que toma señales digitales compuestas de bits, y las transforma en señales analógicas, compuestas de sonidos. También hace el proceso inverso. Se usa para conectar computadoras por teléfono.

+ **Newsgroup** : foro de mensajes públicos en Internet para la discusión de un determinado tema.

+ **Nodo** : computadora parte de una red.

+ **NUA** : Network User Address, dirección del usuario de red. Equivalente del número telefónico en una red de datos X.25.

+ **NUI** : Network User Identification (IUR: Identificación de usuario de red). Numero que identifica a un usuario ante una red X.25.

+ **Numero IP** : identificación de la maquina dentro de la red Internet.

+ **On-Line** : en linea. Significa que algo esta conectado a otra cosa, por lo general una computadora con otra por módem.

+ **Operador** : persona que usa una computadora. A menudo se llama "operador" al administrador del sistema.

+ **Outdial** : módem de salida dentro de una red, que permite a un usuario de la misma salir a la red telefónica convencional. Los que permiten hacer llamadas de larga distancia se llaman "global outdial" (outdial globales) o GOD.

+ **Packet switching** : intercambio de información en forma de paquetes que acumulan una cantidad determinada de bits.

+ **PAD** : Packet Assembler and Disassembler (armador y desarmador de paquetes). Maquina en una red que lee los paquetes y los vuelve a armar, con otro destino o en otro formato. También se llaman asi a las "repetidoras" de una red.

+ **Paper** : trabajo cientifico publicado en forma interna en una universidad o empresa.

+ **Password** : palabra que sirve para verificar que un usuario es realmente quien dice ser. Por esto

mismo, el único que debe conocerla es ese mismo usuario.

+ **Patch** : en inglés, parche. Modificación de un programa ejecutable para solucionar un problema o para cambiar su comportamiento.

+ **Payload** : efecto visible de un software maligno.

+ **PBX** : Private Branch Exchanges. Centrales telefónicas internas de empresas.

+ **Phreaker** : persona que usa comunicaciones sin pagarlas o pagando menos de lo que corresponde.

+ **Pinchar (lineas)** : interferir una linea telefónica (por extensión, cualquier canal de comunicacion) con intenciones de oír lo que se dice o de usar ese canal de comunicación de manera clandestina.

+ **Privilegio** : lo que un sistema deja hacer a un usuario.

+ **Programa** : secuencia de instrucciones para una computadora.

+ **Rabbit** : en inglés, conejo. Programa que provoca procesos inútiles y se reproduce (como los conejos) hasta que agota la capacidad de la máquina.

+ **Recurso** : cualquier cosa que sirva para cumplir las instrucciones (en computadora) de un programa. Puede ser memoria, tiempo de procesamiento, una impresora, un disco, etcétera.

+ **Red Box** : aparato que permite engañar a un teléfono público norteamericano para que se comporte como si se depositaran monedas en él.

+ **Red** : conjunto de computadoras interconectadas que intercambian información.

+ **Redirigir** : cambiar el destino de algo. Por ejemplo, redirigir una llamada es hacer que suene en un teléfono distinto del que se intentaba llamar.

+ **Resetear** : volver un sistema, programa o computadora, a su estado inicial, generalmente apagando y prendiendo la computadora.

+ **Root** : cuenta del administrador en UNIX. Es la mas poderosa: permite el acceso a todo el sistema.

+ **Server** : máquina que ofrece servicios a otras dentro de una red. Véase "host".

+ **Shell** : intérprete de comandos de un sistema operativo. Es el que se encarga de tomar las órdenes del usuario y hacer que el resto del sistema operativo las ejecute.

+ **Shoulder Surfing** : espiar por atrás de un hombro para tratar de ver información interesante.

+ **Sistema operativo** : programa o conjunto de programas que hacen funcionar la máquina. El sistema operativo se encarga de manejar los discos, monitores, terminales, redes, y todo lo que tenga la computadora, mientras que el programa de aplicación pide todo lo que necesita al sistema operativo.

+ **Sistema** : un sistema es cualquier cosa que tenga partes componentes que interactúan entre sí. En computación, se llama así a cualquier conjunto de programas que formen un todo coherente, por ejemplo, dentro de una organización.

+ **Software** : programas para una computadora.

+ **Subir** : enviar un archivo por modem a un host.

+ **Sysop** : administrador de un BBS.

+ **TCP/IP** : conjunto de protocolos usados en la red Internet.

+ **Télex** : red de comunicación de datos muy primitiva, pero todavía en uso. Sirve fundamentalmente para intercambiar mensajes.

+ **Terminal** : puerta de acceso a una computadora. Puede tratarse de un monitor y teclado o de una computadora completa.

+ **Tonos** : los comandos que se usan para controlar las centrales Multifrecuencia telefónicas digitales son tonos audibles. Se los llama multifrecuencia porque cada "tono", o cada señal, es en realidad el resultado de dos sonidos distintos superpuestos. Los tonos que se usan para discar son de este tipo.

+ **Trashing** : arte de revolver la basura para encontrar información útil.

+ **UNIX** : sistema operativo utilizado por la gran mayoría de máquinas de Internet. Su gran éxito se debe a que es abierto, por lo cual existen muchas versiones, y cualquiera puede escribir programas para UNIX.

+ **Virtual** : que no es real. Algo que aparenta ser determinada cosa, pero que en realidad no es mas que una simulación

+ **Virus** : programa autorreproductor que modifica otros programas mientras se reproduce.

+ **Voice** : se dice que una conversación es por voice cuando se usa el teléfono para hablar normalmente en lugar de usar un módem.

+ **Workstation** : estación de trabajo. Es una máquina en la red que se usa para trabajar, a diferencia de un server.

+ **X.25** : protocolo de red packet-switching. Es un estándar internacional usado por la mayoría de las grandes redes.

IX. Bibliografía

Revistas

Secure Computing,

Virus News International,

2600,

The Hacker Quarterly,

Hack-Tic

Wired,

Computer Virus Development Journal,

Whole Earth Review,

Diarios y revistas de Buenos Aires

Virus Report,

Libros:

The Hacker Crackdown: Law and Disorder on The Electronic Frontier, por Bruce Sterling. Bantam Books, 1992.

Los piratas del chip: La mafia informática al desnudo (titulo original: Approaching Zero), por Bryan Clough y Paul Mungo. Ediciones B.S.A., 1992.

Security in Computing, por Charles P. Pfleeger. Prentice Hall International Editions, 1989.

Secrets of a Super Hacker, por The Knightmare. Loompanics Unlimited, 1994.

Neuromante, por William Gibson. Minotauro, 1992.

The Hacker's Dictionary, compilacion de Eric Raymond. The MIT Press, 1991.

Practical UNIX Security, por Simson Garfinkel y Gene Spafford. O'Reilly & Associates, Inc., 1991.

Network Security, por Steven Shaffler y Alan Simon. AP Professional, 1994.

The Internet Worm Program: an Analysis, por Eugene H. Spafford.

A Tour of the Worm, por Donn Seeley.

Firewalls and Internet Security: Repelling the Wily Hacker, por William Cheswick y Steven Bellovin. Addision Wesley Professional Computing, 1994.

A Short Course on Computer Viruses, por Fred Cohen. John Wiley & Sons, Inc.,1994

Out of the Inner Circle, por Bill Landreth. Microsoft Press.

Hackers, por Stephen Levy. Dell Publishing, 1984.

FAQ de alt.2600, por Voyager.